Computational Intelligence for Information Security: A Survey

Ruili Wang and Wanting Ji

***Abstract*—Information security is the set of processes that protect information away from unauthorized access, disclosure, replication, modification, or destruction. Recently, more and more real-world systems such as smart cities, wireless sensor networks, biometric systems, and surveillance, require the assurances of information security. Thus, many different techniques based on computational intelligence have been developed for information security in the past decades. However, there are no comprehensive surveys that summarize these techniques. Thus, this paper reviewed computational intelligence approaches published in journals and conferences for information security in the last decade. This paper is a brief, but a comprehensive survey to review numerous computational intelligence approaches and applications for information security. A discussion of the existing challenges of computational intelligence approaches and techniques for information security is also presented.**

***Index Terms*—Artificial neural networks, computational intelligence, evolutionary computation, fuzzy logic, information security.**

I. Introduction

INFORMATION security is the set of processes that protect information away from unauthorized access, disclosure, replication, modification or destruction [1], [2]. It is designed to maintain Confidentiality, Integrity, and Availability (also known as the CIA triad) of business data (i.e., information) in its various forms [16]. In other words, information security programs are constructed around the core objectives of the CIA triad: 1) ensuring private information is only disclosed to authorized individuals (Confidentiality); 2) preventing unauthorized modifications to private information (Integrity); 3) guaranteeing information is accessed by the authorized individuals when requested (Availability) [2]–[4].

Recently, more and more real-world systems, such as smart cities [5]–[7], wireless sensor networks [8]–[12], and biometric systems [13]–[15], require the assurances of information security. However, the increasing amounts of information and the increasing complexity of information have become major challenges in information security.

Manuscript received November 30, 2018; revised April 24, 2019; accepted June 3, 2019. Date of publication June 22, 2020; date of current version September 23, 2020. This work was supported in part by the China Scholarship Council and in part by the Marsden Fund of New Zealand. *(Corresponding author: Wanting Ji.)*

The authors are with the Zhejiang Gongshang University, Hangzhou 310019, China, and also with the Massey University, Auckland 0632, New Zealand. (e-mail: ruili.wang@massey.ac.nz; jwt@escience.cn).

Digital Object Identifier 10.1109/TETCI.2019.2923426

In order to overcome these challenges, many computational intelligence techniques as well as other machine learning techniques, have been proposed. Machine learning contains a series of widely used data analysis techniques which automates the construction of analytical models [2]. Approaches based on machine learning can (i) learn from data, (ii) identify patterns, and (iii) make decisions with minimal human intervention [3].

Computational intelligence, a sub-field of machine learning, is a study of intelligent mechanisms that can act intelligent behaviors in complex and changing environments [16]–[18]. Specifically, computational intelligence forms a set of nature-inspired computational methodologies and approaches to solving complex real-world data-driven problems that are difficult to solve manually (i.e., through mathematical or traditional modelling) [17], [18].

Computational intelligence combines three core approaches to create intelligent mechanisms: fuzzy logic, artificial neural networks, and evolutionary computation [16]. In addition to these three main approaches, recent computational intelligence encompasses approaches such as the hybrids of the above [16]–[18]. These computational intelligence approaches have been successfully used to solve many problems in information security, such as searching an optimal solution [19], [20], classifying normality and abnormality in an intrusion detection system [21], [22], and data hiding [23]–[25].

In the past decades, various computational intelligence techniques have been developed for information security. However, there are no comprehensive surveys, which review and summarize these techniques. In this paper, over 100 articles, which utilize computational intelligence techniques for information security, are reviewed. These articles are published in journals and conferences in the last ten years.

The contributions of this survey are: 1) presenting a brief, but comprehensive survey to summarize numerous computational intelligence approaches and techniques for information security; 2) discussing existing challenges in computational intelligence approaches for information security.

The rest of this survey is organized as follows. Section II presents the background of information security. Section III reviews the two core approaches of computational intelligence (i.e., fuzzy logic and artificial neural networks) for information security and discusses the strengths and limitations of them in solving information security problems. Section IV reviews evolutionary computation for information security and discusses its advantages and limitations in solving information security problems. Section V summarizes several systems in the real world

2471-285X © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.

TABLE I
DEFINITIONS AND LITERATURE OF INFORMATION SECURITY STRATEGIES

Strategy	Definitions and literature
Prevention	Prevention aims to protect information by preventing unauthorized accesses, disclosure, replication, modification or destruction [4, 33, 155-157].
Surveillance	Surveillance is the systematic monitoring of information, which was designed to perceive environmental developments to adapt to fast-changing environments and threats [34, 161-163].
Detection	Detection is an operational-level strategy, which was designed to identify specific security behaviors [28-30, 164-166].
Response	Response aims to take appropriate corrective operations for identified attacks [4, 31, 167-169].
Deception	Deception utilizes decoys to distract attackers' attention from critical information to cost the attackers' time and resources [32, 170-172].

where computational intelligence approaches have been applied for information security. Section VI is the conclusion arising from this research.

II. BACKGROUND

The aim of information security is to protect information away from unauthorized access, disclosure, replication, modification or destruction, and to maintain the CIA triad of business data (i.e., information) in its various forms [1], [2], [16]. Recently, multiple information security strategies have been defined and classified in a variety of ways, and there is no full consensus on the definition or classification. Ahmad *et al.* [3] summarized a series of information security strategies including prevention, surveillance, detection, response, and deception. These strategies can be used in different situations to keep systems away from unnecessary security risks in order to ensure continuous service access to users. Table I lists the definitions and the literature of these information security strategies. Computational intelligence is often used to implement these strategies. A brief description of these strategies is presented in the following subsections.

A. Prevention

The prevention strategy aims to protect information by preventing unauthorized accesses, disclosure, replication, modification or destruction [4], [33]. Strictly, the prevention strategy has little tolerance for any form of unauthorized individuals. Therefore, this prevention strategy is often used to avoid information leakage.

A common prevention technique is authentication, which was designed to limit the access of unauthorized individuals to information or systems. Further prevention measures such as 1) using software to regulate user interaction with information, 2) encrypting information flowing over networks, 3) using firewalls to filter network traffic, and 4) using anomaly and signature detection paradigms to protect information security also can be used to avoid information leakage.

B. Surveillance

The surveillance strategy is systematic monitoring of information, which was designed to perceive environmental developments to adapt to fast-changing environments and threats [34]. This environmental awareness enables decision makers to better identify information security incidents and develop effective defense measures.

In practice, it is challenging to use a technical or non-technical means to monitor environments, subject to physical and logical space access restrictions. Monitoring typically utilizes visually-available tools or software to store monitored results to enhance decision makers' control of information environments.

C. Detection

The detection is an operational-level strategy, which was designed to identify specific security behaviors [28]–[30]. The purpose of detection is to allow an information system to react in a targeted manner. The detection strategy is much different from the surveillance strategy, which was designed to understand the overall environments. Therefore, the detection strategy only focuses on specific system events whereas the surveillance strategy focuses on the overall status.

The detection strategy can be implemented in a variety of forms, such as the identification of malicious or unusual behavior, as well as specific attacks. In addition, the detection strategy has been used to trigger the operation of suspicious activity collection. Various security measures, such as intrusion detection, network scanning, and anomaly detection, are used in the detection strategy.

D. Response

The response strategy aims to take appropriate corrective operations for identified attacks. The response to an identified attack can be divided into two phases: 1) the reaction phase, in which appropriate corrective operations are taken against the attackers/attacks; 2) the recovery phase, in which the environment will be restored to its original status [31].

A variety of measures can be used for responses when attacked, which depends on how they react to the attack. For example, a reaction is to 'exclude' an attacker by moving the attacker to a different position. The response can be implemented by 1) dropping connections and blocking suspicious IP addresses, or 2) containing, which separates the attacked area from other (unaffected) areas [4].

E. Deception

The deception is a process that taking operations such as enhancement, reduction or distortion to mislead attackers so that the attackers will take (or not take) specific actions to keep information secure. In other words, the deception strategy utilizes decoys to distract attackers' attention from critical information to cost the attackers' time and resources [4], [32]. There are two

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.

types of deception strategy: passive deception and active deception. Passive deception aims to hide whereas active deception focus on the performance.

In information security, the deception strategy was utilized to convince an attacker that the provided information is true information, thereby prompting them to change or expose the attacker's actions to protect the system security. In order to guide an attacker to be deceived, decoys are used to attract the attacker's attention. The deception strategy has proved effective in misdirecting attackers into falsely information systems, in which they can be monitored without compromising the real systems.

III. Computational Intelligence for Information Security

Computational intelligence is a study of intelligent mechanisms that can act intelligent behaviors in complex and changing environments [16]–[18]. Since computational intelligence emerged several decades ago, a variety of approaches have been developed to achieve computational intelligence. The idea of computational intelligence was first mentioned by the IEEE Neural Networks Council in 1990. In 1994, Bezdek proposed the early definition of computational intelligence [33], [34]. He defined computational intelligence as:

> *A system is computationally intelligent if 1) it contains pattern-recognition components and does not use knowledge in the artificial intelligence sense when dealing with low-level data (such as numerical data), 2) it exhibits computational adaptively, fault tolerance, speed approaching human-like turnaround and error rates that are closed to human performance.*

Bezdek also distinguished the differences between computational intelligence and artificial intelligence in [35]. Specifically, computational intelligence processes numeric-level representation whereas artificial intelligence processes symbolic-level representation. Computational intelligence depends on low-level data rather than 'knowledge' whereas artificial intelligence utilizes "knowledge tidbits" [35]–[39]. Meanwhile, facing a problem, computational intelligence operates the given problem in a bottom-up manner whereas artificial intelligence analyses the structure of the given problem in a top-down manner [40]–[42]. In other words, artificial intelligence is about providing engineering solutions to problems that appear intelligent whereas computational intelligence simulates the intelligence of nature to some extent by the use of certain computational approaches, such as fuzzy logic, artificial neural networks, and evolutionary computation [16]–[18].

In following sections, we will review two core approaches of computational intelligence (i.e., fuzzy logic and artificial neural network) for information security and discusses the strengths and limitations of them in solving information security problems.

A. Fuzzy Logic for Information Security

In this section, we will review the contributions and performances of fuzzy logic for information security.

1) Fuzzy Logic: Fuzzy logic is a form of multi-valued logic that aims to formalize approximate reasoning. In a broad sense, fuzzy logic is almost synonymous with fuzzy set theory [43]–[48].

In the crisp set theory, the association between an element and a set is clear and crisp, that is, an element certainly belongs to or does not belong to a set. In some cases, however, the membership is difficult to be precisely measured. For example, a dessert can be described as a good cake. Some people think the cake is sufficiently sweet to be a good cake whereas others think it is too sweet to be a good cake. In other words, we cannot precisely define the sweet degree of a cake or what kind of cake is good. Therefore, the fuzzy set theory has been developed to deal with such uncertainty resulting from imprecise or vague data.

The fuzzy set theory utilized a membership function to define the degree to which an element belongs to a set. The membership degree of objects of a fuzzy set ranges from 0 to 1. Mathematically, let *X* be an ordinary (i.e., crisp) set, and

$$A = \{(x, \mu_A(x)) \,|x \in X\} \;\; with \; \mu_A : X \to [0, 1] \quad (1)$$

is a fuzzy set of *X*. The membership function $\mu_A(x)$ maps the elements in *X* onto real numbers in [0, 1]. A larger value denotes a higher membership degree.

2) Fuzzy Logic for Information Security: Gmach *et al*. [44] proposed an automatic management technique which can provide adaptive service management in different granularities. Specifically, service management consists of three different granularities:

1) Static resource management, which aims to create a service-to-hardware allocation to provide balanced resource utilization. This avoids idle and overload situations when reducing the burden of dynamic resource management;
2) Dynamic resource management, which is based on AutoGlobe [45] and its fuzzy logic based feedback control framework. AutoGlobe provides an up-to-date view of the load situation. Then the fuzzy controller generates actions based on this view to remedying imminent overload, failure, or idle;
3) The adaptive control of Service Level Agreements (SLAs), which intelligently schedule or manage individual changing demand.

However, the proposed technique had difficulties in making fast adaptive adjustments when the load situation suddenly changed (such as a sudden increase in load).

Yu *et al*. [46] proposed an adaptive and automatically tuning the intrusion detection system, which utilized fuzzy reasoning for predicting network intrusions. Specifically, the most suspicious predictions were pushed to the system operator by a prediction filter for verification. When a false prediction was identified, the system automatically tuned the detection model and adjusted the tuning strength based on the feedback of the detection model on earlier data. However, when the system changed drastically or the tuning was delayed too long, the benefits of tuning were reduced or even negative.

Duman *et al.* [49] proposed a Fuzzy-based Intelligent embedded Agents System (F-IAS). Specifically, agents were organized

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.

into societies, in which agents communicated with each other via embedded ambassador agents (i.e., embassadors). Then the embassadors utilized the knowledge they learned to set up connections between agents. Based on the degree of correlations between agent pairs, the embassadors recommended agent associations, which were self-aware and had abilities to reconfigure themselves to react to changes. This process reduced the number of associations and interconnections between various agents in a multi-agent society. Thus, F-IAS can minimize processing latency and overheads to optimize the network.

Acampora *et al*. [50] proposed an interoperable and adaptive fuzzy service for ambient intelligence application based on the multi-agent paradigm and fuzzy logic theory. It created long-life learning strategies to generate context-aware-based fuzzy services and implemented them through semantic Web approaches to maximize users' comfort and hardware interoperability levels.

Bagchi [51] proposed a Fuzzy Adaptive Buffering (FAB) method, which was based on a mobile client-pull model, for buffer management of mobile clients. In order to save battery power and computing resources of mobile clients, FAB utilized a two-thread model and employed fuzzy inference approaches to enhance the total sleeping cycle of data pre-fetch threads. Thus, this method successfully avoided buffer overflow and underflow when maintaining playback quality of multimedia applications and can achieve a smooth user experience. It also proved that fuzzy logic was capable of making decisions based on parameters that are not always clearly stated [115], [116].

Kolomvatsos *et al*. [52] proposed a fuzzy logic system for bargaining in information markets. The fuzzy logic was used to deal with the decision made by a buyer at each stage of the negotiation process. In other words, during the negotiation process, the buyer can make a decision (i.e., accept or reject a seller) based on the following factors: the suggested price, the seller's deadline, the remaining time, and the demand relevancies. However, this system did not consider the buyer's attitude towards risk as well as whether the risk can change the buyer's decision. To solve this limitation, Zhan *et al*. [117] proposed a bargaining system based on fuzzy reasoning. Since a bargainer may change his demand preference during bargaining, the proposed system utilized fuzzy logic to deal with the degree to which the bargainer may change his/her preference. Thus, the chance to reach an agreement can be increased.

Xi *et al*. [53] proposed a fuzzy extractor system, which seamlessly combined biometrics with cryptography, for fingerprint verification. Specifically, the authors developed a bio-crypto-oriented scheme, namely Vertex-indexed Triangulation (ViT), which performs fingerprint verification based on rotation and shift-free minutia local structures. After that, a fuzzy extractor system, namely Fuzzy Extractor based Selective Vertex-indexed Triangulation (FE-SViT), was developed to achieve high verification accuracy with highly parallelizable and efficient.

Tal *et al*. [54] summarized fuzzy logic-based solutions in vehicular networks. Since fuzzy logic was known for its ability in handling complexity, imprecision, and model non-deterministic problems, it can effectively address the challenges in vehicular networks. The authors described fuzzy logic concepts and their applications in vehicular networks, classified and analyzed the fuzzy logic based solutions in vehicular networks, and discussed the utilization of fuzzy logic in some special directions in vehicular networks, such as 5G-enabled vehicular networks.

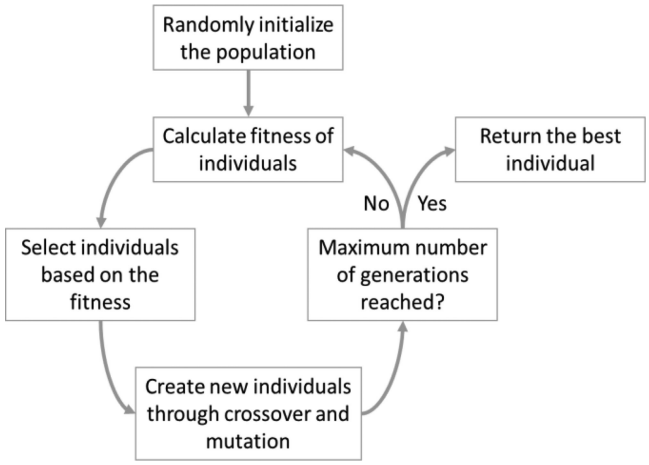


Fig. 1. The process of genetic programming.

Fuzzy Rule Interpolation (FRI) is a process that makes inference possible in sparse rule-based systems and reduces the complexity of fuzzy models. A FRI system can generate a large number of interpolation rules during the interpolation reasoning process. Naik *et al*. [55] proposed a dynamic fuzzy rule interpolation (D-FRI) method for intrusion detection, which utilized the interpolation rules to improve the coverage and efficiency of the whole system.

3) Summary: In general, fuzzy logic or fuzzy set theory provides a flexible way for information security and increases the robustness and adaptive capabilities of information security methods [56]. Currently, there are two main research aims in the study of fuzzy logic: (i) increase the learning and adaptive capabilities of algorithms for automatically designing fuzzy rules; (ii) apply fuzzy logic to machine learning methods (such as support vector machines and hidden Markov models) to enhance the comprehensibility and readability of the methods. Since fuzzy logic has the ability to model the uncertainty of natural languages, it can smooths the abrupt separation between normality and abnormality in an information security system. This is very useful for information security, especially in anomaly detection as well as other applications for information security.

B. Artificial Neural Networks for Information Security

In this section, we will review the contributions and performances of artificial neural networks for information security.

1) Artificial Neural Networks: An artificial neural network consists of a collection of processing units (i.e., neurons) [42]. In an artificial neural network, these processing units interconnected to simulate a neural network of a human brain so that a computer can learn things and make a decision in a humanlike way [57]–[59]. Since these neurons can be highly interconnected in a given topology, artificial neural networks have been successfully applied to a wide range of data-intensive applications.

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.

As shown in Fig. 1, there are three basic components exist in an artificial neural network [17]:

1) Link: Weight W_{ji} is provided to the n inputs of the j^{th} neuron x_i by the links, where $i = 1, \ldots, n$;
2) Aggregation function: The aggregation function sums the weighed inputs as the input to an activation function:

$$u_j = \sum_{i=1}^{n} W_{ji} x_i + b_{ji}, \tag{2}$$

where b_{ji} is the bias, which is a numerical value related to neurons.

2) Activation function: An activation function ψ maps u_j to $v_j = \psi(u_j)$, where v_j is the output value of a neuron. Common activation functions include step, sigmoid, and tan hyperbolic.

2) Artificial Neural Networks for Information Security: A widely use of artificial neural networks for information security is intrusion detection systems. An intrusion detection system is a system for identifying the malicious use of computers or network resources [21]. It aims to monitor and detect possible attacks, including intrusions from outside the system and unauthorized behaviors of internal users, and take appropriate protective measures. Choudhary and Swarup [22] proposed an intrusion detection system based on artificial neural networks, namely Generalized Regression Neural Network (GRNN), to improve the alert throughput of a network. The proposed system can identify attack patterns and their types.

In an image classification task, the classified image may contain sensitive information, such as a passport image containing user personal information. Lorenzi and Vaidya [60] considered that the process of previous classification methods are not safe, and this sensitive information may be stolen during the classification process. Therefore, the authors proposed an image classification method based on artificial neural networks, which can extract sensitive information from a large amount of image data and protect sensitive information from attacks during the classification process.

Malware is a kind of information security risks. A common way of dealing with malware is to manual analyze malware samples by experts. However, such manual analysis requires hours to weeks, depending on the complexity of the malware. In order to solve this problem, Yakura *et al*. [57] proposed a convolutional neural network based method to extract important byte sequences in malware samples. Specifically, a malware sample was converted to an image firstly. Then the converted image was applied to an attention-based convolutional neural network. The network was trained by the images of known malware samples and their labels (i.e., malware family). After that, the network predicted which malware family the malware sample belongs to. Based on the attention map, byte sequences peculiar to the malware can be extracted.

Steganographer detection is a process to identify criminal users, who attempt to hide confidential information through steganography methods, among innocent users. The main challenge of steganographer detection is how to collect evidence to identify guilty users with suspicious images. These suspicious images are embedded with secret messages [58], which are generated by unknown steganography methods and payload. Zheng *et al.* [58] proposed a Multi-class Deep Neural Networks based Steganographer Detection (MDNNSD) method to address this challenge. In the training stage, the proposed network was trained for image classification with six types of embedding payloads (i.e., the payloads are set from 0.1 to 0.5 bit-per-pixel (bpp)). In the testing stage, the learned model extracted features of each image from each user, which can be utilized to distinguish the differences between guilty users and innocent users.

Yang and Eickhoff [59] proposed an embedding model based on feed-forward neural networks. In the proposed model, social network check-ins were transformed into functional, temporal, and geographic information in the form of dense numerical vectors for modelling locations, communities, and users. Moreover, this model can be applied to many real-world applications, such as location recommendation, urban functional zone study, and crime prediction. In location recommendation, a Spatio-Temporal Embedding Similarity algorithm (STES) was proposed based on the model, which can capture item correlations well in terms of activity and location similarities. Although the proposed model showed strong robustness, the structure of the current network was simple, which may have difficulties in mining potential information.

3) Summary: In this section, we reviewed the research in employing artificial neural networks for information security. Since artificial neural networks have the ability in processing limited, noisy, and incomplete data, researchers have taken these advantage to solve information security problems. Moreover, due to the complexity of information security problems and the rise of deep neural networks, more artificial neural networks have been developed and applied to different information security scenarios in information security. Table II summarized the recent work based on deep neural networks for information security.

IV. Evolutionary Computation for Information Security

In this section, we will review the applications of evolutionary computation for information security and discusses its advantages and limitations in solving information security problems.

A. Evolutionary Computation

Biological evolution is an adaptation process that aims to improve survivability through a series of processes such as natural selection, survival of the fittest, reproduction, mutation, competition and symbiosis. Inspired by it, evolutionary computation is an abstraction of biological evolution theory that creates optimization procedures or methodologies and implements them on computers to solve problems.

Evolutionary computation utilizes Darwin's theory of evolution as evolutionary rules and combines Mendel's theory of genetic variation to achieve reproduction, variation, competition and selection in the process of biological evolution. Most evolutionary algorithms contain the following common properties [61]:

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.

TABLE II
DEEP NEURAL NETWORKS FOR INFORMATION SECURITY

Data	Tasks	Deep neural network architectures	References
CFG Graphs	Malware detection	Yolo [123], LeNet-5 [124]	[125]
Images	Alternative Biometrics	Inception V3 [126]	[127]
Images	Counterfeit detection	AlexNet variant [128]	[129]
Images	Defacement detection	AlexNet [128], Denoising Auto-encoder [130]	[130]
Images	Face verification	DeepID2 [131]	[131]
Images	Face verification	SDAE [132], DBM [133]	[133]
Images	Face verification	FaceNet [134]	[134]
Images	Fingerprint orientation field extraction	LeNet-5 variant [124]	[135]
Images	Iris verification	AlexNet variant [128]	[136]
Images	Iris verification	AlexNet [128], Custom CNN [137]	[137]
Images	Liveness detection	VGG19 [138]	[139]
Images	Printer attribution	Custom CNN [140]	[140]
Images	Soft biometrics classification	VGG19 [138]	[141]
Images	Soft biometrics classification	VGGNet variant [142]	[143]
Images	Steg-analysis	Custom CNN [144]	[144]
Images	Steg-analysis	Custom CNN based on [145]	[146]
Speech	Steg-analysis	LSTM-variant [147]	[147]
Speech	Speaker identification	Bi-RNN [148]	[149]
Voice	Speaker identification	AlexNet [128]	[150]
Network traffic	Intrusion detection	VAE-variant [151]	[152]
Wireless network traffic	Intrusion detection	Auto-encoder [153], MLP [153]	[153]
URL-Sequences	Drive-by-attack detection	EDCNN [154]	[154]

1) Population-based stochastic search. A population consists of a group of individuals, each individual represents a solution. An evolutionary algorithm optimizes a problem by initializing a set of solutions and iteratively updating the solutions. By stochastically removing undesired solutions and introducing small random changes, new solutions will be generated to replace the previous one.
2) Recursive iteration. An evolutionary algorithm iteratively searches for optimal solutions in the search space. The search process does not stop until the maximum number of iterations or a preset threshold is reached.
3) Inherent parameters. An evolutionary algorithm has several inherent parameters, such as population size and the maximum number of iterations. These parameters are usually set according to experience.

Algorithm 1 illustrates a general framework of evolutionary computation. In this section, we will review the contributions and performances of evolutionary computation for information security. Evolutionary computation encompasses genetic algorithm, genetic programming, particle swarm optimization, ant colony optimization, and artificial immune system, which are then reviewed separately.

Algorithm 1: General Framework of Evolutionary Computation.

Input: Problem, parameters
Output: Optimal solutions
i: **Begin**
ii: Initialize the size of the population
iii: Search optimal solutions
iv: **for** $i = 1$ to max_iteration do
v: **for** each candidate solution in the population **do**
vi: generate a new solution with random changes evaluate the fitness of the now solution
vii: **end for**
viii: **end for**
ix: Update optimal solutions
x: **End**

1) Genetic Algorithm for Information Security: The genetic algorithm is based on the principles of natural selection, which allows the population of a group of individuals to develop specified selection rules [46], [62]. The most common steps of a genetic algorithm are as follows:

1) Initialize the population *P* by randomly selecting individuals from the search space *S*;
2) Calculate fitness function $f(x_i)$ for individual x_i in *P*;
3) Select individuals in *P* according to the fitness value;
4) Crossover the selected individuals according to the predetermined crossover probability;
5) Individuals in *P* are mutated according to mutation probability;
6) Update *P* with the newly generated individuals;
7) Calculate fitness function $f(x_i)$ for individual x_i in *P*;
8) Repeat (iii)-(vii) until stopping condition satisfied;
9) Return the most fitted individuals in *P*.

Data hiding is an area of information security, which aims to embed secret information into a cover object without causing any perceptual changes. A genetic algorithm is widely used in data hiding.

Using a genetic algorithm, Chang *et al*. [23] proposed a lossless data hiding method for block truncation coding of compressed color images. However, the quality of stego-images is

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.

low and payload capacity is small [112]. Bhowal *et al*. [24] proposed a two-level method for audio steganography. In the first level, an RSA encryption algorithm was used to encrypt a secret message. Then the encrypted message was encoded into audio data using a genetic algorithm based Least Significant Bit (LSB) algorithm. Since the encrypted message bits were embedded into random and higher LSB layers, the robustness against noise was enhanced.

Khodaei and Faez [25] proposed an image hiding method, which utilized LSB substitution to improve stego-image quality. In order to find the best condition in the distribution of image pixels, a genetic algorithm was used to set the parameters of bijective mapping functions. However, in some cases, the proposed method may not be optimal even if the substitution table was good [82], [113].

Tataru *et al*. [63] proposed a steganographic method based on adaptive LSB, in which messages were embedded in a secure manner using Pixel-Value Differencing (PVD) and chaotic sequences. However, the hiding capacity was low when compared with [114]. Jawad and Khan [64] proposed a robust reversible watermarking method to protect relational databases. The genetic algorithm in this method was used to improve watermark capacity and reduce distortion.

Based on a genetic algorithm, Kanan and Nazeri [65] proposed an image steganography scheme with high embedding capacity and tunable visual image quality. The genetic algorithm was utilized to find the best starting point and scanning order so that to maximize the Peak Signal to Noise Ratio (PSNR) of the stego-image. PSNR is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation, which was widely used to measure the effects of image enhancement methods and image hiding methods on image quality. Later, Doğan [66] proposed a data hiding method based on chaos embedded genetic algorithm for colour images, in which multiple chaotic maps are used to perform the randomness of genetic and PSNR was utilized as the fitness function.

In addition, the genetic algorithm also can be used in intrusion detection systems. Hoque *et al*. [67] proposed a genetic algorithm based intrusion detection system, in which a genetic algorithm was used to efficiently detect various types of network intrusions. Desale and Ade [68] proposed a genetic algorithm based feature selection method for an effective intrusion detection system. Using a genetic algorithm and k-centroid clustering, Chakrabarty *et al*. [69] proposed an anomaly-based intrusion detection system, which performed a high detection rate and low false positive rate. In the proposed system, the genetic algorithm can find the ultimate attack type of an intrusion.

2) Genetic Programming for Information Security: Genetic programming is an automatic learning process inspired by biological evolution [17]. It is an effective evolutionary technique and is very popular in solving information security problems. The process of genetic programming is graphically depicted in Fig. 1. Different from Algorithm 1, which illustrates a general framework of evolutionary computation, it is a detailed description of genetic programming.

Weimer *et al*. [70] proposed an automated method for locating and repairing bugs in software by using genetic programming. Once a program fault was discovered, program variants were generated by genetic programming until the newly generated variant both retained the desired functionality and avoids the defects.

Suarez-Tangil *et al*. [71] proposed a genetic programming based method for automatic generation of security event correlation rules. The genetic programming was used to build optimized Open Source Security Information Management rules. Bazarganigilani *et al*. [72] proposed an optimized method for web crawling. Genetic programming was used to improve the accuracy of measuring web page similarity. Carvalho *et al*. [73] proposed a genetic programming method to record deduplication. The genetic programming has the ability to automatically obtain adaptive deduplication functions, freeing the user from the burden of selecting and tuning parameters.

In cybersecurity, Folino and Pisani [74] proposed a distributed genetic programming framework to evolve a function for combining the classifiers composing the ensemble. Later, Folino *et al*. [75] proposed an ensemble model to classify streaming intrusion detection datasets. The genetic programming was utilized to generate the combiner function of the ensemble model. Malhotra *et al*. [76] proposed a genetic programming and k-nearest neighbor classifier based intrusion detection model. Genetic programming was used to convert pre-processed data into the optimal features that are suitable for classification.

3) Particle Swarm Optimization for Information Security: Particle swarm optimization is a population-based stochastic optimization algorithm that simulates social behavior to achieve precise objectives in multi-dimensional search space [77], [78]. Similar to other evolutionary algorithms, particle swarm optimization performs searches using a population of individuals that are iteratively updated [79]. However, particle swarm optimization does not utilize selection. In other words, all individuals in the population survive from the beginning to the end.

In particle swarm optimization, a population consists of a group of particles (i.e., individuals) in a D-dimensional search space, $X_i = (x_{i1}, x_{i2}, \ldots, X_{iD})$ represents the *i*th particle, $P_i = (p_{i1}, p_{i2}, \ldots, p_{iD})$ represents the best previous position of the *i*th particle, $V_i = (v_{i1}, v_{i2}, \ldots, v_{iD})$ represents the rate of position change (i.e., velocity) of the *i*th particle [65]. The velocities and positions of the particles are changed according to (3) and (4), respectively:

$$v_{id} = v_{id} + c_1^* rand()^* (p_{id} - x_{id}) + c_2^* Rand()^* (p_{gd} - x_{id}), \tag{3}$$

$$x_{id} = x_{id} + v_{id}, \tag{4}$$

where c_1 and c_2 represent positive constants, *rand*()() and *Rand*()() represent two random functions in the range [0, 1]. Common steps of a particle swarm optimization are as follows:

1) Randomly initialize a population of particles with random positions and velocities in a D-dimensional search space;
2) Calculate the desired optimization fitness function $f(x_i)$ for each particle;
3) Calculate the velocity of each particle with (3);

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.

4) Move each particle to the new position according to (4);
5) Repeat (ii)-(iv) until stopping condition satisfied;
6) Return the most fitted individual.

One application area of particle swarm optimization for information security is data hiding. Fazli and Kiamini [19] proposed a steganographic method to embed a secret message into a cover image. In order to improve the quality of stego-image and increase the protection level, this method splits the cover image into n-blocks and the secret message into n-partitions. For each block, a particle swarm optimization algorithm searches approximate optimal solutions and finds an optimal substitution matrix to transform the secret message before embedding.

Rabevohitra and Sang [20] proposed a steganographic method for JPEG compressed image. In order to improve the quality of the stego-image, a particle swarm optimization algorithm was used to find an optimal substitution matrix for transforming the secret message. Nickfarjam and Azimifar [80] proposed a method for image steganography. For each host image, this method defined a special secret key by using particle swarm optimization, and each particle represented a potential solution.

Gerami *et al*. [81] proposed a method that utilized particle swarm optimization to find the optimal pixel position so that to convert a secret image into a new secret image. Then the Optimal Pixel Adjustment (OPA) method was applied to the proposed method to improve the quality of the generated image and reduce image distortion. Compared with the developed method in [118], which utilized the genetic algorithm for image hiding, the proposed method has a higher PSNR value and was robust to chi-square attacks.

Bedi *et al*. [82] proposed a spatial domain based image hiding method that utilized particle swarm optimization to find optimal pixel locations in a grayscale image, where the secret grayscale image pixel can be embedded. Since the pixels used for data hiding were not randomly selected, the quality of the stego-image can be higher than the previous methods [119], [120], [113]. However, it has been proved that this method was not secure against statistical attacks [121], [122].

El-Emam [83] proposed an adaptive neural network based on modified particle swarm optimization for data hiding. It aimed to increase the amount of hiding data, which was embedded in a color image without being perceived and was effective against attacks such as visual attacks and statistical attacks.

Meanwhile, particle swarm optimization was widely used to reduce the computational complexity of a multi-level thresholding problem. Kurban *et al*. [84] compared multiple evolutionary computation approaches (including genetic algorithm, particle swarm optimization, *etc*.) for the multi-level color image thresholding problem. Experimental results demonstrated that particle swarm optimization was more accurate and robust than other evolutionary algorithms in the statistical analysis of objective values, but it required more running time.

4) Ant Colony Optimization for Information Security: Ant colony optimization is a multi-agent system, which is inspired by the behavior of real ant colonies. A real ant can leave pheromones on the ground in order to mark the routes from the nest to food. Other members of the same colony can smell the pheromones, and when choosing routes, they tend to choose the route marked by strong pheromone concentrations. In the absence of pheromones, ants initially choose routes randomly. After a period of time, the shorter routes will be visited more frequently and on these routes, more pheromones will be accumulated. As a result, more ants will choose these routes in the future. This positive feedback means that all ants will choose the shortest route in the end [85]–[87].

In ant colony optimization, each individual of the population is an agent that can build a solution to a problem gradually [85]. Agents build solutions to the problem by moving on a graph-based representation. In each step, the movement defined the solution components that added to the population. Therefore, the optimal solution can be obtained.

Watermarking is an application area of ant colony optimization for information security. Al-Qaheri *et al*. [86] proposed a watermarking embedding and retrieval method using ant colony optimization, in which ant colony optimization was utilized to enhance the robustness of the retrieval process.

Loukhaoukha *et al*. [87] proposed an optimal watermarking method, which was based on lifting wavelet transform and singular value decomposition, using multi-objective ant colony optimization. The singular values of a binary watermark were embedded in the sub-band of an image. In order to increase the robustness without losing the transparency of the watermark, multiple scaling factors, the optimal values of which were determined by multi-objective ant colony optimization, was utilized. Later, Loukhaoukha replaced lifting wavelet transform with a discrete wavelet transform for watermarking in [88] since it had the advantage of low calculation complexity.

Feng *et al*. [89] proposed a Security Risk Analysis Model (SRAM) based on Bayesian networks and ant colony optimization for information systems. Ant colony optimization was used to calculate the vulnerability propagation path and provide guidance for developing security risk treatment plans.

In addition, since feature selection is an important part of machine learning [90]–[94], ant colony optimization can be used to select features for intrusion detection system effectively. Aghdam *et al*. [95] proposed a feature selection method using ant colony optimization in intrusion detection systems. Since ant colony optimization had the ability to converge quickly, this method used it to reduce the dimension of features and to find minimal feature subset in the process of intrusion detection.

5) Artificial Immune System for Information Security: The artificial immune system is inspired by the biological immune system, and demonstrates lots of intelligence, including self-learning, self-adaptation, self-regulation, and distributed self/non-self-detecting capabilities [96]. Specifically, it attempts to identify unknown agents from self-nodes, transmit signals about intrusions in self-nodes, and finally confront these agents by ending their power to eliminate the danger. Similar to biological immune systems that have the ability to fight pathogens, artificial immune systems can be used to protect computers from threats. Therefore, artificial immune systems are widely used for anomaly detection for information security.

Powers and He [97] proposed a hybrid artificial immune system and self-organizing map for network intrusion detection. Specifically, an artificial immune system was used to detect

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.

anomalous network connections. Then the connections which were tagged as anomalous were categorized using a Kohonen self-organizing map. This allowed higher-level information about the detected anomalies can be extracted.

Hosseinpour *et al*. [98] proposed an intrusion detection system by using the idea of artificial immune systems. In this system, an unsupervised innate immune mechanism was developed to primarily categorize network traffic into self (i.e., normal profiles) and non-self (i.e., suspicious profiles), without previous training or knowledge about network flow profiles. Thus, this system can provide online and real-time training for an adaptive immune system within an artificial immune system.

Saurabh and Verma [96] proposed an Efficient Proactive Artificial Immune System based Anomaly Detection and Prevention System (EPAADPS). EPAADPS embodied immune properties and distinguished between self and non-self, for identifying and preventing invisible anomalies.

Suliman *et al*. [99] proposed a network intrusion detection system using an artificial immune system to detect the occurrence of intrusion in a computer network. There were many features, such as duration, protocol type, and service type, in the connection process of a computer network. By classifying the combination of different connection features, the intrusion detection system can distinguish between valid connections and attack connections.

Besides, the authenticity of handwritten signatures is required to be verified in many aspects of current life, such as contract signing, bank transaction, and financial transactions. Serdouk *et al*. [100] proposed a histogram-based descriptor to characterize off-line signatures. The authenticity of these signatures was verified using a joint use of artificial immune recognition system with a support vector machine.

6) Summary: In this section, we reviewed the research of evolutionary computation for information security. Evolutionary computation plays an important role in solving information security problems. For example, genetic algorithms can be used for searching an optimal solution in the population, genetic programming can be used for classifying normality and abnormality in an intrusion detection system, and particle swarm optimization has the ability in data hiding.

Additionally, we also found that evolutionary computation still has challenges in solving information security problems. For example, KDD99-10 dataset [101] is a common dataset for intrusion detection, where there are 391,458 instances in the DoS class and only 52 instances in the U2R class. In other words, the data is distributed unbalanced in this dataset. However, in some cases, the individuals that had better performance on frequently occurring connection types are more likely to survive, even if they performed worse than competing individuals on the less frequent types [102], [103]. Such challenges need to be addressed to enhance the performance of evolutionary computation for information security.

V. Computation Intelligence Applications in System Security

Recently, more and more systems in the real world require the assurances of information security, such as smart cities [5]–[7], wireless sensor networks [8]–[12], and biometric systems [13]–[15]. Unlike the applications mentioned above, these systems require a combination of multiple computation intelligence approaches to ensure information security. In this section, we will review several systems, in which computation intelligence approaches are used to protect the application system security.

A. Smart Cities

With the development in the Internet of Things, smart city has become a trend, which applies a variety of advanced approaches, such as ubiquitous sensing, heterogeneous network infrastructure, and intelligent information processing and control system. A smart city enables real-time monitoring and provides people with intelligent services in transportation, healthcare, environment, entertainment and energy [104], [105]. However, some security and privacy problems arise, since smart city applications not only collect a variety of privacy-sensitive information from people but also control urban facilities and affect people's lives. Thus, how to solve these security and privacy problems in a smart city becomes very important.

There are a large number of data storage devices in smart cities. In some cases, physical damage to these devices can result in data corruption. One solution to this is to monitor these devices from physical damage. Tao *et al*. [5] proposed a method based on Large Substitution Area (GAR) for deploying network monitors to locate damaged devices (i.e., compromised data sources), in which an improved genetic algorithm was developed to achieve optimal deployment.

In smart healthcare, the security of data (e.g., medical images) transmitted over networks needs to be protected. Pareek and Patidar [6] proposed an encryption method for grayscale medical image protection. The proposed method was based on features of a genetic algorithm since the processes (i.e., population, crossover, and mutation) the genetic algorithm can increase the robustness of the method.

Recently, cloud computing based healthcare management systems are considered as an effective way to manage healthcare data and have been applied to smart cities. Thus, the security of medical data becomes an important challenge, including access to medical data and retrieval/management of medical records. Thangarasu *et al*. [7] proposed a biometrically based signature authentication method for cloud healthcare data security, in which an artificial neural network was used for the accuracy of retrieving clinical data onto the cloud. The proposed neural network acquired the biometric signature through a biometric sensor processed with a quality checker for effective authentication [7].

B. Wireless Sensor Networks

A wireless sensor network enables the collection of real-time information by the dense deployment of low-energy and low-cost tiny nodes [106], [107]. Currently, this network is one of the most effective approaches for performing sensing tasks. Over the past decades, wireless sensor networks were beneficial in many areas, the application of such networks has expanded steadily,

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.

from environmental management to industrial control, from structural health monitoring to strategic monitoring [108]–[110].

Wireless sensor networks are susceptible to physical attacks and unauthorized access by malicious users due to some reasons, such as the radio range of the network, untrusted transmission, and unattended nature. Thus, security has become a fundamental requirement for these networks.

The first problem in wireless sensor networks is how to prevent unauthorized access while ensuring information integrity and confidentiality. Li and Parker [8] proposed an intruder detection system that utilized an unsupervised fuzzy Adaptive Resonance Theory (ART) neural network to detect threats in wireless sensor networks. Dhurandher *et al*. [9] proposed a Quality-based Distance Vector routing proposal (QDV) for securing wireless sensor networks by using an ant colony optimization. The ant colony optimization was utilized to distinguish the nodes were reliable or malicious in a wireless sensor network.

In [10], an intrusion detection system was proposed based on the integration of neural network using Genetic Algorithm-Levenberg-Marquardt Algorithm (GA-LMBP) for wireless sensor networks. The proposed system took advantage of offline learning neural networks to build a detection system and offered high true positive detection rates and low power consumption.

In order to ensure the confidentiality of information in wireless sensor networks, Biswas *et al*. [11] proposed a lightweight block cipher by using a chaotic map and genetic programming. The confidentiality of information in the wireless sensor network was provided by an encryption process, which combined the benefits of elliptic curve operations, chaotic mapping, and genetic cryptography. Genetic programming was used since they can introduce a relatively fair diversity in the ciphertext.

Multipath routing is a solution to protect data transmission security in wireless sensor networks. Recently, Gupta *et al*. [12] proposed a genetic algorithm based multipath routing method for wireless sensor networks. The proposed method maximized the fitness function of the genetic algorithm based on the distance between a sending node and a receiving node, the distance between the next hop node to a base station (i.e., a transfer node which was used to prepare routing schedule), and the hop counted from the next hop node to the base station.

C. Biometric Systems

A biometric system is an identification system based on a person's physical or behavioral characteristics [111]. Compared to traditional token-based or knowledge-based systems, biometric systems are able to map identity (i.e., authorized user and unauthorized user) directly to the owner. In addition, biometric systems are easier to use and have lower maintenance costs than other systems.

Currently, since more and more biometric systems were applied in the real world, how to ensure the security and confidentiality of biometric data became a problem. For example, in a fingerprint biometric system, unauthorized users falsifying fingerprints into the system would jeopardize the privacy of system users. Therefore, it is important to improve the safety and integrity of biometric data.

Web automated scanners help web application administrators find vulnerabilities without any knowledge of cybersecurity. Cao *et al*. [13] proposed an ant colony optimization method for establishing detail correspondences by using local descriptors and neighbor propagations in deformed or distorted fingerprints. Specifically, minutiae similarities were considered as heuristic values in ant colony optimization, which can be measured by their orientation descriptors and local minutiae structures.

Kumar *et al*. [14] proposed a bimodal hand knuckle verification system by using ant colony optimization based fuzzy binary decision tree. This system can meet a wide range of applications varying from civilian to high-security areas since it utilized ant colony optimization to select optimal fusion parameters for each level of security.

In [15], a fingerprint recognition framework named DarkHunter was proposed, which can classify different fingerprints of automated web scanners. The proposed framework consists of three components: 1) feature data collection, 2) raw data processing, and 3) feature classification. Specifically, a docker based distributed scanner data collection structure was designed to collect feature data. Then a model named state window was developed to split raw data (i.e., scanner weblogs). Finally, a convolutional neural network based classifier was utilized to identify which scanner the feature data came from. A limitation of DarkHunter was that the framework cannot be dynamically enhanced. It is because the framework is based on convolutional neural networks, in which the size of the training set was fixed before training. Once the training process was completed, new training data cannot be used to improve classification accuracy.

D. Summary

This section explored computation intelligence approaches in protecting the security of real-world application systems. Sections III and IV only summarized how a single computation intelligence approach (e.g., ant colony optimization) can be applied to a particular application (e.g., watermarking). However, a single computation intelligence approach cannot solve all real-world information security problems. Thus, in this section, a particular application has been extended to an application system, and multiple computation intelligence approaches are integrated to protect information security and system security.

VI. Discussion and Conclusion

Over the past decade, information security based on computational intelligence approaches and techniques has been a popular studied topic, which is widely used to satisfy the growing demand for reliable and intelligent systems.

This paper systematically reviewed numerous computational intelligence approaches and techniques for information security. We reviewed more than 170 journal and conference papers on information security published in the past decade. These papers were categorized and summarized according to the computational intelligence approaches utilized and their application areas. Additionally, the existing challenges of computational

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.

intelligence approaches for information security have been discussed.

In our view, these approaches and techniques contribute to information security in different ways:

1) Fuzzy logic represents and processes numeric information in a linguistic format so that the system complexity can be easily managed by mapping a large numerical input space into a small search space. Moreover, the use of linguistic variables has the ability to present normal or abnormal behavior patterns in a readable and easily understandable format. The uncertainty and imprecision of fuzzy logic smooth the sudden separation of normal and abnormal data, thus enhancing the robustness of information security.
2) Other approaches such as artificial neural networks and evolutionary computation were developed from natural inspirations. By introducing "intelligence" via biological metaphors, these approaches have the ability to infer behavior patterns from data without prior knowledge of regularities in the data, thus enhancing the robustness of information security.

Currently, computational intelligence approaches have been widely used in the field of information security and have achieved good performances. In the future, as more and more scenarios/systems require information security, it is necessary to develop more advanced computational intelligence approaches and techniques. We expected that computational intelligence approaches continue to be developed and its applications in information security continue to be expanded. We do hope that this survey can benefit scholars involved in this area. Our future work will focus on a more in-depth analysis of computational intelligence approaches for information security.

REFERENCES

[1] J. Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Amsterdam, the Netherlands: Syngress, 2014.

[2] S. Thaler, V. Menkovski, and M. Petkovic, "Deep learning in information security," 2018, *arXiv:1809.04332*.

[3] A. Ahmad, S. B. Maynard, and S. Park, "Information security strategies: Towards an organizational multi-strategy perspective," *J. Intell. Manuf.*, vol. 25, no. 2, pp. 357–370, Apr. 2014.

[4] S. Liu, J. Sullivan, and J. Ormaner, "A practical approach to enterprise IT security," *IT Prof.*, vol. 5, pp. 35–42, Sep./Oct. 2001.

[5] M. Tao, K. Ota, and M. Dong, "Locating compromised data sources in IoT-enabled smart city: A great-alternative-region-based approach," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2579–2587, Jan. 2018.

[6] N. K. Pareek and V. Patidar, "Medical image protection using genetic algorithm operations," *Soft Comput.*, vol. 20, no. 2, pp. 763–772, Feb. 2016.

[7] G. Thangarasu, P. D. D. Dominic, K. Subramanian, and S. Smiley, "Biometric based signature authentication scheme for cloud healthcare data security," in *Proc. Int. Conf. Reliable Inf. Commun. Technol.*, 2018, pp. 557–565.

[8] Y. Y. Li and L. E. Parker, "Intruder detection using a wireless sensor network with an intelligent mobile robot response," in *Proc. Int. Conf. Southeastcon.*, Apr. 2008, pp. 37–42.

[9] S. K. Dhurandher, S. Misra, M. S. Obaidat, and N. Gupta. "An ant colony optimization approach for reputation and quality-of-service-based security in wireless sensor networks," *Secur. Commun. Netw.*, vol. 2, no. 2, pp. 215–224, Mar. 2009.

[10] F. Lu and L. Wang, "Intrusion detection system based on integration of neural network for wireless sensor network," *J. Softw. Eng.*, vol. 8, pp. 225–238, 2014.

[11] K. Biswas, V. Muthukkumarasamy, and K. Singh, "An encryption scheme using chaotic map and genetic operations for wireless sensor networks," *IEEE Sensors J.*, vol. 15, no. 5, pp. 2801–2809, May 2015.

[12] S. K. Gupta, P. Kuila, and P. K. Jana, "Energy efficient multipath routing for wireless sensor networks: A genetic algorithm approach," in *Proc. Int. Conf. Adv. Comput. Commun. Inf.*, 2016, pp. 1735–1740.

[13] K. Cao, X. Yang, X. Chen, Y. Zang, J. Liang, and J. Tian, "A novel ant colony optimization algorithm for large-distorted fingerprint matching," *Pattern Recognit.*, vol. 45, no. 1, pp. 151–161, Jan. 2012.

[14] A. Kumar, M. Hanmandlu, and H. M. Gupta, "Ant colony optimization based fuzzy binary decision tree for bimodal hand knuckle verification system," *Expert Syst. Appl.*, vol. 40, no. 2, pp. 439–449, Feb. 2013.

[15] Y. Fang, X. Long, L. Liu, and C. Huang, "DarkHunter: A fingerprint recognition model for web automated scanners based on CNN," in *Proc. 2nd Int. Conf. Cryptography Secur. Privacy*, 2018, pp. 10–15.

[16] R. Iqbal, F. Doctor, B. More, S. Mahmud, and U. Yousuf, "Big data analytics: Computational intelligence techniques and application areas," *Technol. Forecasting Social Change*, pp. 1–13, 2018. [Online]. Available: https://doi.org/10.1016/j.techfore.2018.03.024

[17] R. V. Kulkarni, A. Forster, and G. K. Venayagamoorthy, "Computational intelligence in wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 1, pp. 68–96, Mar. 2011.

[18] E. M. El-Alfy, and W. S. Awad, "Computational intelligence paradigms: An overview," in *Proc. Improving Inf. Secur. Pract. Through Comput. Intell.*, 2016, pp. 1–27.

[19] S. Fazli and M. Kiamini "A high performance steganographic method using JPEG and PSO algorithm," in *Proc. Int. Conf. IEEE Multitopic*, 2008, pp. 100–105.

[20] F. H. Rabevohitra and J. Sang, "High capacity steganographic scheme for JPEG compression using particle swarm optimization," *Adv. Mater. Res.*, vol. 433, pp. 5118–5122, 2012.

[21] S. Sonawane, S. Karsoliya, P. Saurabh, and B. Verma, "Self configuring intrusion detection system," in *Proc. 4th Int. Conf. Comput. Intell. Commun. Netw.*, 2012, pp. 757–761.

[22] A. K. Choudhary and A. Swarup, "Neural network approach for intrusion detection," in *Proc. 2nd Int. Conf. Interact. Sci. Inf. Technol. Culture Human*, 2009, pp. 1297–1301.

[23] C. Chang, C. Lin, and Y. Fan, "Lossless data hiding for color images based on block truncation coding," *Pattern Recognit.*, vol. 41, no. 7, pp. 2347–2357, Jul. 2008.

[24] K. Bhowal, A. J. Pal, G. S. Tomar, and P. P. Sarkar, "Audio steganography using GA," in *Proc. Int. Conf. Comput. Intell. Commun. Netw.*, 2010, pp. 449–453.

[25] M. Khodaei and K. Faez, "Image hiding by using genetic algorithm and LSB substitution," in *Proc. Int. Conf. Image Signal Process.*, Berlin, Germany, 2010, pp. 404–411.

[26] R. Baskerville, P. Spagnoletti, and J. Kim, "Incident-centered information security: Managing a strategic balance between prevention and response," *Inf. Manage.*, vol. 51, no. 1, pp. 138–151, Jan. 2014.

[27] R. Appleby and R. N. Anderton, "Millimeter-wave and submillimeter-wave imaging for security and surveillance," *Proc. IEEE*, vol. 95, no. 8, pp. 1683–1690, Aug. 2007.

[28] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Proc. Int. Conf. IEEE Wireless Mobile Comput. Netw. Commun.*, 2005, vol. 3, pp. 253–259.

[29] W. Lee and D. Xiang, "Information-theoretic measures for anomaly detection," in *Proc. Int. Symp. IEEE Secur. Privacy*, 2001, pp. 130–143.

[30] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The value of intrusion detection systems in information technology security architecture," *Inf. Syst. Res.*, vol. 16, no. 1, pp. 28–46, Mar. 2005.

[31] J. D'Arcy, T. Herath, and M. K. Shoss, "Understanding employee responses to stressful information security requirements: A coping perspective," *J. Manage. Inf. Syst.*, vol. 31, no. 2, pp. 285–318, Oct. 2014.

[32] H. Chen *et al.*, "Coplink center: Social network analysis and identity deception detection for law enforcement and homeland security intelligence and security informatics: A crime data mining approach to developing border safe research," in *Proc. Nat. Conf. Digital Government Res.*, 2005, pp. 112–113.

[33] N. Siddique and H. Adeli, "Computational intelligence: Synergies of fuzzy logic," in *Neural Networks and Evolutionary Computing*. New York, NY, USA: Wiley, 2013.

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.

[34] H. Kumar, "Computational intelligence approach for flow shop scheduling problem," in *Handbook of Research on Emergent Applications of Optimization Algorithms*. Hershey, PA, USA: IGI Global, 2018, pp. 298–313.
[35] J. C. Bezdek, "Intelligence: Computational versus artificial," *IEEE Trans. Neural Netw.*, vol. 4, no. 5, pp. 737–747, Sep. 1993.
[36] J. C. Bezdek, "On the relationship between neural networks, pattern recognition and intelligence," *Int. J. Approx. Reason.*, vol. 6, no. 2, pp. 85–107, Feb. 1992.
[37] J. C. Bezdek, "Computational intelligence defined-by everyone!" in *Computational Intelligence: Soft Computing and Fuzzy-Neuro Integration with Applications*. Berlin, Germany: Springer, 1998, pp. 10–37.
[38] J. Fulcher, "Computational intelligence: An introduction," in *Computational Intelligence*. Berlin, Germany: Springer, 2008, pp. 3–78.
[39] J. C. Bezdek, "What is computational intelligence?" *Comput. Intell.-Imitating Life*, pp. 1–12, 1994.
[40] B. C. Craenen and A. E. Eiben, "Computational intelligence," *Encyclopedia of Life Support Sciences*, EOLSS Publishers Co., Ltd., Oxford, U.K., 2002.
[41] W. Duch, "What is computational intelligence and where is it going?" in *Challenges for Computational Intelligence*. Berlin, Germany: Springer, 2007, pp. 1–13.
[42] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," *Appl. Soft Comput.*, vol. 10, no. 1, pp. 1–35, Jan. 2010.
[43] L. A. Zadeh, "Fuzzy logic, neural networks, and soft computing," in *Fuzzy Sets, Fuzzy Logic, and Fuzzy System*. Singapore: World Scientific, 1996, pp. 775–782.
[44] D. Gmach, S. Krompass, A. Scholz, M. Wimmer, and A. Kemper, "Adaptive quality of service management for enterprise services," *ACM Trans. Web*, vol. 2, no. 1, Feb. 2008, Art. no. 8.
[45] S. Seltzsam, D. L. Gmach, S. Krompass, and A. Kemper, "Autoglobe: An automatic administration concept for service-oriented database applications," in *Proc. 22nd Int. Conf. Data Eng.*, 2006, Art. no. 90.
[46] L. A. Zadeh, "Fuzzy logic = computing with words," *IEEE Trans. Fuzzy Syst.*, vol. 4, no. 2, pp. 103–111, May 1996.
[47] J. Lu and R. Wang, "An enhanced fuzzy linear regression model with more flexible spreads," *Fuzzy Sets Syst.*, vol. 160, no. 17, pp. 2505–2523, Sep. 2009.
[48] Y. Zeng, M. Zhou, and R. Wang, "Similarity measure based on nonlinear compensatory model and fuzzy logic inference," in *Proc. Int. Conf. IEEE Granular Comput.*, 2005, pp. 342–345.
[49] H. Duman, H. Hagras, and V. Callaghan, "A multi-society-based intelligent association discovery and selection for ambient intelligence environments," *ACM Trans. Auton. Adaptive Syst.*, vol. 5, no. 2, May 2010, Art. no. 7.
[50] G. Acampora, M. Gaeta, V. Loia, and A. V. Vasilakos, "Interoperable and adaptive fuzzy services for ambient intelligence applications," *ACM Trans. Auton. Adaptive Syst.*, vol. 5, no. 2, May 2010, Art. no. 8.
[51] S. Bagchi, "A fuzzy algorithm for dynamically adaptive multimedia streaming," *ACM Trans. Multimedia Comput., Commun. Appl.*, vol. 7, no. 2, Feb. 2011, Art. no. 11.
[52] K. Kolomvatsos, C. Anagnostopoulos, and S. Hadjiefthymiades, "A fuzzy logic system for bargaining in information markets," *ACM Trans. Intell. Syst. Technol.*, vol. 3, no. 2, Feb. 2012, Art. no. 32.
[53] K. Xi, J. Hu, and B. V. K. Kumar, "FE-SViT: A SViT-based fuzzy extractor framework," *ACM Trans. Embedded Comput. Syst.*, vol. 15, no. 4, Sep. 2016, Art. no. 78.
[54] I. Tal and G. M. Muntean, "Towards reasoning vehicles: A survey of fuzzy logic-based solutions in vehicular networks," *ACM Comput. Surveys*, vol. 50, no. 6, Dec. 2017, Art. no. 80.
[55] N. Naik, R. Diao, and Q. Shen, "Dynamic fuzzy rule interpolation and its application to intrusion detection," *IEEE Trans. Fuzzy Syst.*, vol. 26, no. 4, pp. 1878–1892, Aug. 2018.
[56] N. Goel and M. Kaur, "A review of soft computing techniques in biometrics," in *Proc. 2nd Int.Conf. Recent Adv. Eng. Comput. Sci.*, 2015, pp. 1–4.
[57] H. Yakura, S. Shinozaki, R. Nishimura, Y. Oyama, and J. Sakuma, "Malware analysis of imaged binary samples by convolutional neural network with attention mechanism," in *Proc. 8th ACM Conf. Data Appl. Secur. Privacy*, 2018, pp. 127–134.
[58] M. Zheng, S. Zhong, S. Wu, and J. Jiang, "Steganographer detection based on multiclass dilated residual networks," in *Proc. Int. Conf. ACM Multimedia Retrieval*, 2018, pp. 300–308.
[59] J. Yang and C. Eickhoff, "Unsupervised learning of parsimonious general-purpose embeddings for user and location modeling," *ACM Trans. Inf. Syst.*, vol. 36, no. 3, pp. 1–33, Mar. 2018.
[60] D. Lorenzi and J. Vaidya, "Identifying a critical threat to privacy through automatic image classification," in *Proc. 1st ACM Conf. Data Appl. Secur. Privacy*, 2011, pp. 157–168.
[61] A. Emrouznejad, *Big Data Optimization: Recent Developments and Challenges*, vol. 18. New York, NY, USA: Springer, 2016.
[62] Z. Yu, J. J. Tsai, and T. Weigert, "An adaptive automatically tuning intrusion detection system," *ACM Trans. Auton. Adaptive Syst.*, vol. 3, no. 3, Aug. 2008, Art. no. 10.
[63] R. L. Tataru, D. Battikh, S. El Assad, H. Noura, and O. Déforges, "Enhanced adaptive data hiding in spatial LSB domain by using chaotic sequences," in *Proc. 8th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2012, pp. 85–88.
[64] K. Jawad and A. Khan, "Genetic algorithm and difference expansion based reversible watermarking for relational databases," *J. Syst. Softw.*, vol. 86, no. 11, pp. 2742–2753, Nov. 2013.
[65] H. R. Kanan and B. Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm," *Expert Syst. Appl.*, vol. 41, no. 14, pp. 6123–6130, Oct. 2014.
[66] Ş. Doğan, "A new data hiding method based on chaos embedded genetic algorithm for color image," *Artif. Intell. Rev.*, vol. 46, no. 1, pp. 129–143, Jun. 2016.
[67] M. S. Hoque, M. Mukit, M. Bikas, and A. Naser, "An implementation of intrusion detection system using genetic algorithm," *Int. J. Netw. Secur. Appl.*, vol. 4, no. 2, pp. 109–120, 2012.
[68] K. S. Desale and R. Ade, "Genetic algorithm based feature selection approach for effective intrusion detection system," in *Proc. Int. Conf. Comput. Commun. Inf.*, 2015, pp. 1–6.
[69] B. Chakrabarty, O. Chanda, and M. S. Islam, "Anomaly based intrusion detection system using genetic algorithm and k-centroid clustering," *Int. J. Comput. Appl.*, vol. 163, no. 11, pp. 13–17, 2017.
[70] W. Weimer, T. V. Nguyen, C. L. Goues, and S. Forrest, "Automatically finding patches using genetic programming," in *Proc. 31st Int. Conf. Softw. Eng.*, 2009, pp. 364–374.
[71] G. S. Tangil, E. Palomar, J. M. Fuentes, J. Blasco, and A. Ribagorda, "Automatic rule generation based on genetic programming for event correlation," in *Computational Intelligence in Security for Information Systems*. Berlin, Germany: Springer, 2009, pp. 127–134.
[72] M. Bazarganigilani, A. Syed, and S. Burki, "Focused web crawling using decay concept and genetic programming," *Int. J. Data Mining Knowl. Manage. Process.*, vol. 1, no. 1, pp. 1–12, Jan. 2011.
[73] M. G. Carvalho, A. H. Laender, M. A. Gonçalves, and A. S. Silva, "A genetic programming approach to record deduplication," *IEEE Trans. Knowl. Data Eng.*, vol. 24, no. 3, pp. 399–412, Mar. 2012.
[74] G. Folino and F. S. Pisani, "Combining ensemble of classifiers by using genetic programming for cyber security applications," in *Proc. Eur. Conf. Appl. Evol. Comput.*, 2015, pp. 54–66.
[75] G. Folino, F. S. Pisani, and P. Sabatino, "An incremental ensemble evolved by using genetic programming to efficiently detect drifts in cyber security datasets," in *Proc. Int. Conf. Genetic Evol. Comput.*, 2016, pp. 1103–1110.
[76] S. Malhotra, V. Bali, and K. K. Paliwal, "Genetic programming and K-nearest neighbor classifier based intrusion detection model," in *Proc. 7th Int. Conf. Cloud Comput., Data Sci. Eng.*, 2017, pp. 42–46.
[77] D. Qiu, Y. Li, X. Zhang, and B. Gu, "Support vector machine with parameter optimization by bare bones differential evolution," in *Proc. 7th Int. Conf. Nat. Comput.*, 2011, vol. 1, pp. 263–266.
[78] M. He, M. Liu, R. Wang, X. Jiang, B. Liu, and H. Zhou, "Particle swarm optimization with damping factor and cooperative mechanism," *Appl. Soft Comput.*, vol. 76, pp. 45–52, Mar. 2019.
[79] T. K. Das, G. K. Venayagamoorthy, and U. O. Aliyu, "Bio-inspired algorithms for the design of multiple optimal power system stabilizers: SPPSO and BFA," *IEEE Trans. Ind. Appl.*, vol. 44, no. 5, pp. 1445–1457, Sep. 2008.
[80] A. M. Nickfarjam and Z. Azimifar, "Image steganography based on pixel ranking and particle swarm optimization," in *Proc. 16th CSI Int. Symp. Artif. Intell. Signal Process.*, 2012, pp. 360–363.
[81] P. Gerami, S. Ebrahim, and M. Bashardoost, "Least significant bit image steganography using particle swarm optimization and optical pixel adjustment," *Int. J. Comput. Appl.*, vol. 55, no. 2, pp. 20–25, 2012.

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.

[82] P. Bedi, R. Bansal, and P. Sehgal, "Using PSO in a spatial domain based image hiding scheme with distortion tolerance," *Comput. Elect. Eng.*, vol. 39, no. 2, pp. 640–654, Feb. 2013.

[83] N. N. El-Emam, "New data-hiding algorithm based on adaptive neural networks with modified particle swarm optimization," *Comput. Secur.*, vol. 55, pp. 21–45, Nov. 2015.

[84] T. Kurban, P. Civicioglu, R. Kurban, and E. Besdok, "Comparison of evolutionary and swarm based computational techniques for multilevel color image thresholding," *Appl. Soft Comput.*, vol. 23, pp. 128–143, Oct. 2014.

[85] M. Dorigo and M. Birattari, "Ant colony optimization," in *Encyclopedia of Machine Learning*. Boston, MA, USA: Springer, 2011, pp. 36–39.

[86] H. Al-Qaheri, A. Mustafi, and S. Banerjee, "Digital watermarking using ant colony optimization in fractional Fourier domain," *J. Inf. Hiding Multimed. Signal Process.*, vol. 1, no. 3, pp. 179–189, Jul. 2010.

[87] K. Loukhaoukha, J. Y. Chouinard, and M. H. Taieb, "Optimal image watermarking algorithm based on LWT-SVD via multi-objective ant colony optimization," *J. Inf. Hiding Multimed. Signal Process.*, vol. 2, no. 4, pp. 303–319, Oct. 2011.

[88] K. Loukhaoukha, "Image watermarking algorithm based on multiobjective ant colony optimization and singular value decomposition in wavelet domain," *J. Optim.*, vol. 2013, pp. 1–10, Jun. 2013.

[89] N. Feng, H. J. Wang, and M. Li, "A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis," *Inf. Sci.*, vol. 256, pp. 57–73, Jan. 2014.

[90] R. Wang *et al.*, "Review on mining data from multiple data sources," *Pattern Recognit. Lett.*, vol. 109, no. 15, pp. 120–128, Jul. 2018.

[91] P. Yi, A. Song, J. Guo, and R. Wang, "Regularization feature selection projection twin support vector machine via exterior penalty," *Neural Comput. Appl.*, vol. 28, no. 1, pp. 683–697, Dec. 2017.

[92] S. S. Tirumala, S. R. Shahamiri, A. S. Garhwal, and R. Wang, "Speaker identification features extraction methods: A systematic review," *Expert Syst. Appl.*, vol. 90, pp. 250–271, Dec. 2017.

[93] J. Guo, P. Yi, R. Wang, Q. Ye, and C. Zhao, "Feature selection for least squares projection twin support vector machine," *Neurocomputing*, vol. 144, pp. 174–183, Nov. 2014.

[94] W. Ji, R. Wang, and J. Ma, "Dictionary-based active learning for sound event classification," *Multimed. Tools Appl.*, vol. 78, no. 3, pp. 3831–3842, 2018. [Online]. Available: https://doi.org/10.1007/s11042-018-6380-z

[95] M. H. Aghdam and P. Kabiri, "Feature selection for intrusion detection system using ant colony optimization," *Int. J. Netw. Security*, vol. 18, no. 3, pp. 420–432, May 2016.

[96] P. Saurabh and B. Verma, "An efficient proactive artificial immune system based anomaly detection and prevention system," *Expert Syst. Appl.*, vol. 60, pp. 311–320, Oct. 2016.

[97] S. T. Powers and J. He, "A hybrid artificial immune system and self-organizing map for network intrusion detection," *Inf. Sci.*, vol. 178, no. 15, pp. 3024–3042, Aug. 2008.

[98] F. Hosseinpour, P. V. Amoli, F. Farahnakian, J. Plosila, and T. Hämäläinen, "Artificial immune system based intrusion detection: innate immunity using an unsupervised learning approach," *Int. J. Digital Content Technol. Appl.*, vol. 8, no. 5, pp. 1–12, Oct. 2014.

[99] S. I. Suliman, M. S. A. Shukor, M. Kassim, R. Mohamad, and S. Shahbudin, "Network intrusion detection system using artificial immune system (AIS)," in *Proc. 3rd Int. Conf. Comput. Commun. Syst.*, 2018, pp. 178–182.

[100] Y. Serdouk, H. Nemmour, and Y. Chibani, "A new handwritten signature verification system based on the histogram of templates feature and the joint use of the artificial immune system with SVM," in *Proc. IFIP Int. Conf. Comput. Intell. Appl.*, Oran, Algeria, May 2018, pp. 119–127.

[101] S. D. Bay, D. Kibler, M. J. Pazzani, and P. Smyth, "The UCI KDD archive of large data sets for data mining research and experimentation," *ACM SIGKDD Explorations Newslett.*, vol. 2, no. 2, pp. 81–85, Dec. 2000.

[102] H. H. Dam, K. Shafi, and H. A. Abbass, "Can evolutionary computation handle large datasets? A study into network intrusion detection," in *Proc. Australasian Joint Conf. Artif. Intell.*, Berlin, Germany, 2005, pp. 1092–1095.

[103] D. Song, M. I. Heywood, and A. N. Z. Heywood, "A linear genetic programming approach to intrusion detection," in *Proc. Genetic Evol. Comput. Conf.*, Berlin, Germany, 2003, pp. 2325–2336.

[104] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.

[105] N. K. Suryadevara, S. C. Mukhopadhyay, R. Wang, R. K. Rayudu, and Y. M. Huang, "Reliable measurement of wireless sensor network data for forecasting wellness of elderly at smart home," in *Proc. Int. Conf. IEEE Instrum. Meas. Technol.*, 2013, pp. 16–21.

[106] R. W. Anwar *et al.*, "Security issues and attacks in wireless sensor network," *World Appl. Sci. J.*, vol. 30, no. 10, pp. 1224–1227, Nov. 2014.

[107] N. K. Suryadevara, S. C. Mukhopadhyay, R. Wang, and R. K. Rayudu, "Forecasting the behavior of an elderly using wireless sensors data in a smart home," *Eng. Appl. Artif. Intell.*, vol. 26, no. 10, pp. 2641–2652, Nov. 2013.

[108] T. Chen, R. Wang, B. Dai, D. Liu, and J. Song, "Likelihood-field-model-based dynamic vehicle detection and tracking for self-driving," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 11, pp. 3142–3158, Nov. 2016.

[109] Y. Fang, L. Sun, H. Fu, T. Wu, R. Wang, and B. Dai. "Learning deep compact channel features for object detection in traffic scenes," in *Proc. Int. Conf. IEEE Image Process.*, 2016, pp. 1052–1056.

[110] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 266–282, May 2014.

[111] M. Douglas, K. Bailey, M. Leeney, and K. Curran, "An overview of steganography techniques applied to the protection of biometric data," *Multimed. Tools Appl.*, vol. 77, no. 13, pp. 17333–17373, Jul. 2018.

[112] N. N. El-Emam and R. A. S. Al-Zubidy, "New steganography algorithm to conceal a large amount of secret message using hybrid adaptive neural networks with modified adaptive genetic algorithm," *J. Syst. Softw.*, vol. 86, no. 6, pp. 1465–1481, Jun. 2013.

[113] P. Bedi, R. Bansal, and P. Sehgal, "Using PSO in image hiding scheme based on LSB substitution," in *Proc. Int. Conf. Adv. Comput. Commun.*, Berlin, Germany, 2011, pp. 259–268.

[114] N. Sathisha, K. S. Babu, K. B. Raja, and K. R. Venugopal, "Image steganography using non embedding and average technique in transform domain," *Int. J. Sci. Eng. Res.*, vol. 6, no. 1, pp. 920–928, Jan. 2015.

[115] G. Cueva-Fernandez, J. P. Espada, V. García-Díaz, and R. Gonzalez-Crespo, "Fuzzy decision method to improve the information exchange in a vehicle sensor tracking system," *Appl. Soft Comput.*, vol. 35, pp. 708–716, Oct. 2015.

[116] C. González García, E. R. Núñez-Valdez, V. García-Díaz, G. Pelayo, B. C. Bustelo, and J. M. C. Lovelle, "A review of artificial intelligence in the internet of things," *Int. J. Interactive Multimed. Artif. Intell.*, vol. 5, no. 4, pp. 1–12, Mar. 2019.

[117] J. Zhan, X. Luo, K. M. Sim, C. Feng, and Y. Zhang, "A fuzzy logic based model of a bargaining game," in *Proc. Int. Conf. Knowl. Sci., Eng. Manage.*, Berlin, Germany, 2013, pp. 387–403.

[118] M. Wu, M. Lin, and C. Chang, "A LSB substitution oriented image hiding strategy using genetic algorithms," in *Proc. Adv. Workshop Content Comput.*, Berlin, Germany, 2004, pp. 219–229.

[119] I. Lin, Y. Lin, and C. Wang, "Hiding data in spatial domain images with distortion tolerance," *Comput. Standards Interfaces*, vol. 31, no. 2, pp. 458–464, Feb. 2009.

[120] R. Bajaj, P. Bedi, and S. K. Pal, "Best hiding capacity scheme for variable length messages using particle swarm optimization," in *Proc. Int. Conf. Swarm Evol. Memetic Comput.*, Berlin, Germany, 2010, pp. 230–237.

[121] T. Zhang, W. Li, Y. Zhang, and X. Ping, "Detection of LSB matching steganography based on distribution of pixel differences in natural images," in *Proc. Int. Conf. Image Anal. Signal Process.*, 2010, pp. 548–552.

[122] H. Wu, N. Wu, C. Tsai, and M. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *IEE Proc., Vis. Image Signal Process.*, vol. 152, no. 5, pp. 611–615, Oct. 2005.

[123] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: Unified, real-time object detection," in *Proc. Int. Conf. IEEE Comput. Vis. Pattern Recog.*, 2016, pp. 779–788.

[124] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proc. IEEE*, vol. 86, no. 11, pp. 2278–2324, Nov. 1998.

[125] M. H. Nguyen, D. L. Nguyen, X. M. Nguyen, and T. T. Quan, "Auto-detection of sophisticated malware using lazy-binding control flow graph and deep learning," *Comput. Secur.*, vol. 76, pp. 128–155, Jul. 2018.

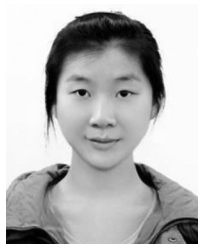
[126] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in *Proc. Int. Conf. IEEE Comput. Vis. Pattern Recognit.*, 2016, pp. 2818–2826.

[127] M. Azimpourkivi, U. Topkara, and B. Carbunar, "A secure mobile authentication alternative to biometrics," in *Proc. Annu. Conf. Comput. Secur. Appl.*, 2017, pp. 28–41.

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.

[128] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *Proc. Adv. Neural Inf. Process. Syst.*, 2012, pp. 1097–1105.
[129] A. Sharma, V. Srinivasan, V. Kanchan, and L. Subramanian, "The fake vs real goods problem," in *Proc. ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2017, pp. 2011–2019.
[130] K. Borgolte, C. Kruegel, G. Vigna, K. Borgolte, C. Kruegel, and G. Vigna, "Meerkat: Detecting website defacements through image-based object recognition," in *Proc. 24th USENIX Conf. Security*, 2015, pp. 595–610.
[131] Y. Sun, Y. Chen, X. Wang, and X. Tang, "Deep learning face representation by joint identification-verification," in *Proc. 27th Int. Conf. Neural Inf. Process. Syst.*, 2014, pp. 1988–1996.
[132] P. Vincent, H. Larochelle, Y. Bengio, and P. Manzagol, "Extracting and composing robust features with denoising autoencoders," in *Proc. Int. Conf. Mach. Learn.*, 2008, pp. 1096–1103.
[133] G. Goswami, M. Vatsa, and R. Singh, "Face verification via learned representation on feature rich video frames," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1686–1698, Jul. 2017.
[134] F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," in *Proc. Int. Conf. IEEE Comput. Vis. Pattern Recognit.*, 2015, pp. 815–823.
[135] K. Cao and A. K. Jain, "Latent orientation field estimation via convolutional neural network," in *Proc. Int. Conf. Biometrics*, 2015, pp. 349–356.
[136] H. Proença and J. C. Neves, "Deep-PRWIS: Periocular recognition without the iris and sclera using deep learning frameworks," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 4, pp. 888–896, Apr. 2018.
[137] Z. Zhao and A. Kumar, "Accurate periocular recognition under less constrained environment using semantics-assisted convolutional neural network," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1017–1030, May 2017.
[138] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014, *arXiv:1409.1556*.
[139] R. F. Nogueira, R. D. A. Lotufo, and R. C. M. Hado, "Fingerprint liveness detection using convolutional neural networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1206–1213, Jun. 2016.
[140] A. Ferreira *et al.*, "Data-driven feature characterization techniques for laser printer attribution," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1860–1873, Aug. 2017.
[141] N. Narang and T. Bourlai, "Gender and ethnicity classification using deep learning in heterogeneous face recognition," in *Proc. Int. Conf. Biometrics*, 2016, pp. 1–8.
[142] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep face recognition," in *Proc. Brit. Mach. Vis. Conf.*, 2015, vol. 1, Art. no. 41.
[143] E. Gonzalez-Sosa, J. Fierrez, R. Vera-Rodriguez, and F. Alonso-Fernandez, "Facial soft biometrics for recognition in the wild: Recent works, annotation, and COTS evaluation," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2001–2014, Aug. 2018.
[144] J. Ye, J. Ni, and Y. Yi, "Deep learning hierarchical representations for image steganalysis," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2545–2557, Nov. 2017.
[145] G. Xu, H. Wu, and Y. Shi, "Structural design of convolutional neural networks for steganalysis," *IEEE Signal Process. Lett.*, vol. 23, no. 5, pp. 708–712, May 2016.
[146] J. Zeng, S. Tan, B. Li, and J. Huang, "Large-scale JPEG image steganalysis using hybrid deep-learning framework," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1200–1214, May 2018.
[147] Z. Lin, Y. Huang, and J. Wang, "RNN-SM: Fast steganalysis of VoIP streams using recurrent neural network," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1854–1868, Jul. 2018.
[148] M. Schuster and K. K. Paliwal, "Bidirectional recurrent neural networks," *IEEE Trans. Signal Process.*, vol. 45, no. 11, pp. 2673–2681, Nov. 1997.
[149] E. C. R. Shin, D. Song, and R. Moazzezi, "Recognizing functions in binaries with neural networks," in *Proc. USENIX Secur. Symp.*, 2015, pp. 611–626.
[150] L. Uzan and L. Wolf, "I know that voice: Identifying the voice actor behind the voice," in *Proc. Int. Conf. Biometrics*, 2015, pp. 46–51.
[151] D. P. Kingma and M. Welling, "Auto-encoding variational Bayes," 2014, *arXiv:1312.6114*.
[152] G. Osada, K. Omote, and T. Nishide, "Network intrusion detection based on semi-supervised variational auto-encoder," in *Proc. Eur. Symp. Res. Comput. Secur.*, Cham, Switzerland, 2017, pp. 344–361.
[153] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 621–636, Mar. 2018.
[154] T. Shibahara *et al.*, "Malicious URL sequence detection using event denoising convolutional neural network," in *Proc. Int. Conf. IEEE Commun.*, 2017, pp. 1–7.
[155] V. Virta, "The red team toolbox, a method for penetration tests," in *Proc. Eur. Inst. Comput. Antivirus Res. Conf.*, 2005, pp. 1–5.
[156] H. T. Ray, R. Vemuri, and H. R. Kantubhukta, "Toward an automated attack model for red teams," *IEEE Security Privacy*, vol. 3, no. 4, pp. 18–25, Jul. 2005.
[157] B. W. Lampson, "Computer security in the real world," *Computer*, vol. 37, no. 6, pp. 37–46, Jun. 2004.
[158] R. Roman, J. Lopez, and S. Gritzalis, "Situation awareness mechanisms for wireless sensor networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 102–107, Apr. 2008.
[159] K. K. Stouffer and J. Falco, "Recommended practices: Improving industrial control systems cybersecurity with defense-in-depth strategies," *Dept. Homeland Secur., Control Syst. Secur. Program, Nat. Cyber Secur. Division*, Washington, DC, USA, 2009.
[160] P. Barford *et al.*, "Cyber SA: Situational awareness for cyber defense," in *Cyber Situational Awareness*. Boston, MA, USA: Springer, 2010, pp. 3–13.
[161] M. R. Stytz, "Considering defense in depth for software applications," *IEEE Security Privacy*, vol. 2, no. 1, pp. 72–75, Jan. 2004.
[162] E. E. Eilertson, L. Ertoz, V. Kumar, and K. S. Long, "MINDS: A new approach to the information security process," *Army High Performance Comput. Res. Center*, Minneapolis, MN, USA, pp. 1–5, 2004.
[163] H. Debar and E. Tombini, "Accurate detection of HTTP attack traces in web server logs," in *Proc. Eur. Inst. Comput. Antivirus Res.*, Saint Julians, Malta, Apr. 2005, pp. 1–5.
[164] D. Armstrong, S. Carter, G. Frazier, and T. Frazier, "Autonomic defense: Thwarting automated attacks via real-time feedback control," *Complexity*, vol. 9, no. 2, pp. 41–48, Nov. 2003.
[165] O. S. Saydjari, "Cyber defense: Art to science," *Commun. ACM*, vol. 47, no. 3, pp. 52–57, Mar. 2004.
[166] M. M. Williamson, "Resilient infrastructure for network security," *Complexity*, vol. 9, no. 2, pp. 34–40, Nov. 2003.
[167] N. C. Rowe, "Counterplanning deceptions to foil cyber-attack plans," in *Proc. IEEE Syst. Man Cybern. Soc. Inf. Assurance Workshop*, 2003, pp. 203–210.
[168] N. C. Rowe, E. J. Custy, and B. T. Duong, "Defending cyberspace with fake honeypots," *J. Comput.*, vol. 2, no. 2, pp. 22–36, 2007.
[169] N. C. Rowe, "Measuring the effectiveness of honeypot counter-counterdeception," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2006, vol. 6, Paper 129c.

Ruili Wang received the Ph.D. degree in computer science from Dublin City University, Dublin, Ireland. He is a Professor of artificial intelligence at Massey University, Auckland, New Zealand. His current research interests include machine learning, language and speech processing, image and video processing, and computer vision. He has published more than 137 papers, of which 95 are in peer-reviewed journals. He has supervised 18 Ph.D. to completion. He is an Associate Editor (or an editorial board member) for the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE, *Neurocomputing* (Elsevier), *Knowledge and Intelligent Systems* (Springer), *Applied Soft Computing* (Elsevier), *Health Information Science and System* (Springer), and *Complex and Intelligent Systems* (Springer). He was the recipient of the Marsden Grant in 2013 in machine learning and its application to speech processing.



Wanting Ji received the B.E. and M.E. degrees from Liaoning University, Shenyang, China, in 2013 and 2016, respectively. She is currently working toward the Ph.D. degree at Massey University, Auckland, New Zealand. Her current research interests include signal processing, video processing, and machine learning.

Authorized licensed use limited to: Massey University. Downloaded on July 28,2021 at 09:36:01 UTC from IEEE Xplore. Restrictions apply.