IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 22, 2020, accepted December 3, 2020, date of publication December 14, 2020,
date of current version December 29, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.3044453*

# Artificial Intelligence Aided Electronic Warfare Systems- Recent Trends and Evolving Applications

**PURABI SHARMA[1], KANDARPA KUMAR SARMA[1], (Senior Member, IEEE), AND NIKOS E. MASTORAKIS[2], (Senior Member, IEEE)**

[1]Department of Electronics and Communication Engineering, Gauhati University, Guwahati 781014, India
[2]Department of Industrial Engineering, Technical University of Sofia, 1000 Sofia, Bulgaria

Corresponding author: Purabi Sharma (purabis1989@gmail.com)

This work was supported by TEQIP - MHRD, Government of India.

**ABSTRACT** Electronic warfare (EW) is one of the most important characteristics of modern battles. EW can affect a military force's use of the electromagnetic spectrum to detect targets or to provide information. Recent developments in artificial intelligence (AI) suggest that this emerging technology will have a deterministic and potentially transformative influence on military power. AI driven algorithms can be very effective in diverse domain of EW like processing of radar signals for efficient recognition and classification of emitters, detection of jammer and its characteristics and for developing efficient anti-jamming algorithms. AI techniques can also enable an EW system to operate autonomously. This paper provides a description of various branches of EW, the role of AI in EW systems and different AI techniques that have been deployed in EW systems.

**INDEX TERMS** Artificial intelligence, deep neural network, ECM, electronic warfare, ESM, ECCM, jamming.

## I. INTRODUCTION

Modern military forces are heavily dependent on a variety of complex and continuously evolving technologies for effective war-fighting capability using electronic means [1]. Electronic Warfare (EW) is a specialized set of tools that assists air, land, naval, and space forces at multiple levels of conflict by putting restrictions on the use of the radio frequency (RF) spectrum. Nowadays, defence forces pay particular attention to the development and improvement of their assets, systems and complexes for EW [2]. Despite achieving significant enhancement of war-fighting capability due to employment of EW, optimization of utilization of resources and efficient decision support continues to be major issues in military operations. Application of artificial intelligence (AI) along with EW has been regarded to be an option that has the potential to bridge the gap between the desired war-fighting capability and the acquired skills. World over, EW and AI have been accepted to form a combination which shall play decisive roles in ensuring defeat and victory. AI has already been regarded to be essential for mobile EW systems deployed along with battlefield formations [3]. The primary reasons behind the preference for the use of AI based EW systems are the capability of efficient decision support, handling large amounts of data, situational awareness, visualization of the evolving scenario and generation of appropriate responses. Moreover, military systems equipped with AI have better self-control, self-regulation, and self-actuation due to its inherent computing and decision-making capabilities [4]. This paper focuses on the description of fundamental aspects of EW and its components, different elements and related technology of the present generation of EW systems, application of AI as an aid for effective deployment and decision making in the battlefield and evolving scenario of AI aided EW which shall be crucial for military forces in the days ahead.

## II. BACKGROUND

It is an established fact that EW systems have a direct influence on the information space of military conflict. Concurrently, AI techniques are being investigated to determine their value as a component of a new, improved EW system so that the optimal and efficient use of resources is bolstered. In this direction, many AI-based techniques have been proposed to improve the performance of an EW system [5]–[9]. To continue with this description, the definition of EW, the

The associate editor coordinating the review of this manuscript and approving it for publication was Weipeng Jing.

subdivision of EW system and fundamentals of AI, and the relevant techniques are described in the following subsections.

### A. ELECTRONIC WARFARE (EW)

EW is any military action that involves the use of the entire electromagnetic spectrum to intercept, analyze and manipulate the enemy's use of the spectrum while protecting one's own effective use of the same spectrum. The objective of EW is to determine the existence of the enemy's electronic aids as part of war-fighting capability, destroy the effectiveness of the enemy's electronic warfare aids and to deny the destruction of the effectiveness of friendly EW resources. EW represents a set of techniques used to deny free access to the electromagnetic spectrum. These techniques are adopted for denying services rendered by the communication system and radar based methods used as a part of military setups. EW consists of three major subdivisions: Electronic Attack (EA), Electronic Protection (EP), and Electronic Warfare Support (ES) systems. EA refers to the actions taken to prevent or reduce the enemy's effective use of the electromagnetic spectrum. EP involves actions taken to protect the effective use of the electromagnetic spectrum for friendly forces. ES comprises of all those measures taken to detect, intercept, locate and analyse sources of radiated electromagnetic energy. So, all of the three components of EW must be carefully integrated to be effective. The subdivisions of EW are described below.

#### 1) ELECTRONIC WARFARE SUPPORT (ES)

ES or Electronic Support Measures (ESM) in general, involves methods of gathering EW information through Electronic intelligence (ELINT), Communication Intelligence (COMINT), and ESM receiver. The key functions of ESM systems are: intercepting, identifying, analyzing, and locating sources of hostile electromagnetic radiation for the purposes of immediate threat recognition and the tactical employment of military forces or assets, such as ECM equipment. Moreover, ES information correlated with other intelligence surveillance information can be developed into an electronic order of battle (EOB) for situational awareness. This information can also be used to develop new countermeasures. Hence, ESM is an important EW information source to carry out ECM and ECCM operations. The main objective of an ELINT system is to compile operational data on enemy electronic systems and weapons. COMINT is the intelligence derived from unfriendly communication by persons other than the intended recipients. The Combination of ELINT and COMINT is called signal intelligence (SIGINT). Both ESM and SIGINT operate in the electromagnetic spectrum and use the same electromagnetic resources. The main difference between ESM and SIGINT is that ESM function is for a tactical purpose that requires immediate actions, whereas SIGINT collects intelligence data for subsequent or non real-time analysis [10].

The ESM system basically measures the parameters of the incoming radar signal in the operating frequency range. The typical parameters are: pulse width, pulse repetition frequency (PRF), signal power, time of arrival (TOA), the direction of arrival (DOA), etc [8]. The ESM system normally consists of: Antennas, Receivers, Signal processor, Computer with emitter library and Display unit [11].

An antenna is a specialized transducer that converts the received RF signal into a suitable form and sends it to the front-end receiver. The principal function of an ESM receiver is to provide information regarding the existence and nature of various signals in the minimum possible time. ESM receiver identifies the usable intelligence carried by the signal (i.e., frequency, PRF, pulse width, scan type and rate, polarisation, amplitude) and measures the DOA of the waveform so as to calculate the location of the transmitter. Signal processor process and preserve the signal characteristics for later in-depth analysis and provide significant information to the operator for making intelligent and timely decisions. The display unit obtains the track data file from the ESM processor and displays the emitter details on the screen.

ESM receiver has the largest influence on the characteristics of the ESM system [12]. There are various receiver approaches to achieve the desired characteristics for the system. Radar warning receiver (RWR) is an example of an ESM system that intercepts radar signals and analyzes their relative threat in real-time [13]. RWR have a threat library in its microprocessor that represents the enemy EOB. The performance of a simple RWR deteriorates when many radar emitters are present in the dense environment [14]. In such situations, there arises a requirement of filtering or sorting of emissions in order to classify each signal so as to extract the important parameters like the amplitude, pulse width, frequency, angle of arrival (AOA), coherency, polarisation, pulse train characteristics, etc. of the radar.

Based on various design approach, some important advance ESM receivers that have excellent multiple signal handling capability even in a dense emitter environment as discussed in [10] are:

- Crystal Video Receiver (CVR): This is a small-sized, low-cost receiver that is excellent for limited application. However, their capability is limited to fine frequency measurement and cannot readily handle complex and dense signals. They have poor sensitivity and are incapable of handling frequency agile systems.
- Superheterodyne receivers: The advantage of these receivers is that they have high sensitivity, better frequency selectivity, proven design, and are not susceptible to jamming. However, this type of receiver has a poor probability of intercept if the emitter is frequency agile or frequency hopping.
- Microscan receiver: This type of receiver has the advantage of a high probability of detection. Also, they are capable of handling the wideband and frequency agile signals efficiently. But the drawback with this type of receiver is that they require a channelizer, minimum

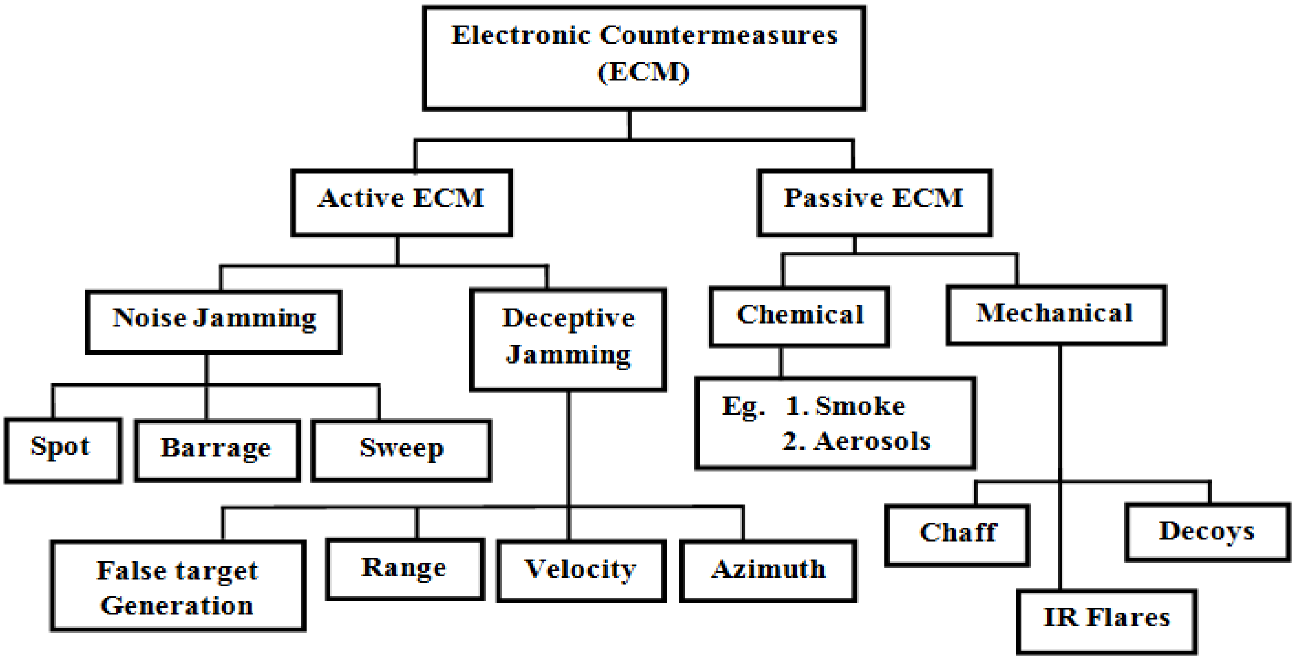

**FIGURE 1.** Different methods of ECM.

pulse width, multiple receivers for direction finding operations, and a very wide IF bandwidth.

- Channelized receivers: This type of receiver has high selectivity and a high probability of detection and is not susceptible to jamming. But the shortcoming of this receiver is that they require a channeliser, thereby increasing the receiver's size and cost.
- Instantaneous frequency measurement (IFM) receivers: The advantage of this type of receiver is that they have a high probability of detection and good frequency measurement accuracy. They can also handle frequency agile signals efficiently. However, they have the limitations of poor sensitivity, easy jamming, inability to handle a very high data rate, and continuous wave signals.

### 2) ELECTRONIC ATTACK (EA)

EA, also known as Electronic Countermeasures (ECM), is the component of EW that involves the use of electromagnetic energy or anti-radiation weapons to attack personnel or equipment with the intent of neutralizing or destroying enemy combat capability. The main operational objectives of ECM are:

- To prevent hostile ESM and communication systems from receiving information regarding the operation of friendly forces within the radar coverage.
- To introduce pseudo, deceptive data into hostile electronic systems in order to generate ineffective personnel or command and control actions.
- To destroy hostile electronic warfare system so as to deny the destruction of friendly EW resources.

Various ECM techniques that are used to prevent or reduce the enemy's effective use of the electromagnetic spectrum are shown in Figure 1.

The two major techniques of ECM are Active ECM and Passive ECM [13], [15]. Active ECM involves degradation of effectiveness of the enemy's electronic warfare aids by generating and transmitting electromagnetic energy. It involves two major actions, namely noise jamming and deceptive jamming [13]. Jamming prevents threat radar from measuring target position and velocity, whereas deception techniques produce false position and velocity of the target. Jamming is the deliberate radiation of electromagnetic energy to weaken the use of electronic devices and systems. Noise jamming attempts to inject an interference signal into the enemy's electronic system such that the target signal is masked or completely submerged by interference. There are three different techniques for generating noise-like IF interference [16]:

- **Spot Jamming**: In this type of jamming, all the power of the jammer is concentrated to a very narrow band of frequencies which should ideally be that of the radar.
- **Sweep Jamming**: In this type of jamming, the jammer sweeps its frequency from one to other over a very wide bandwidth.
- **Barrage Jamming**: In this type of jamming, the jammer targets multiple frequencies simultaneously. All the power of the jammer is spread over a bandwidth much wider than that of the radar signal and hence overcomes the challenges associated with other types of jamming.

In the deception jamming technique, the ECM systems deliberately deceive the radar and send out pseudo signals to mislead the hostile systems in deriving interpretation of information received by their electronic system. Deception can be either manipulative or imitative [14]. Modification of friendly electromagnetic radiations to accomplish deception is called manipulative deception. Introducing radiation into enemy channels that mimic their own emission is called imitative deception. Deception jamming can be broadly classified into four categories, namely false target generation, range deception, velocity deception, and angle deception [12], [16].

- **False target generation**: This is an effective jamming technique employed against acquisition, early warning, and ground control intercept (GCI) radars. The objective of this type of jamming is to confuse the enemy radar operator by generating many false target returns on the victim radar [10]. When this technique is successfully employed, the radar operator cannot distinguish between false targets and real targets [15].
- **Range deception**: In this technique, range deception jammer exploits any inherent weakness in missile guiding radar system's automatic range gate tracking circuits. When the distance between the real and false targets is larger than the range gate of the radar, the deceptive jammer shuts down.
- **Velocity deception**: Continuous wave (CW) radar and Pulse Doppler radar track targets based on velocity or Doppler-shifted frequency. In this deception technique, the velocity tracking information is denied by generating pseudo velocity targets. This is accomplished by using techniques like velocity gate pull-off (VGPO), Doppler noise, narrowband Doppler noise.
- **Angle deception**: In this technique, jammer degrades the tracking radar's ability to extract the correct angle and elevation information of a target. So, radar acquires incorrect information about the angular position of the target. Based on different angle measurement algorithms, there are many angle deception techniques. Such as for conical scan radars, scan rate modulation and inverse gain jamming is used, for Lobe-On-Receive-Only (LORO) tracking radars, swept square wave (SSW) jamming is used, for monopulse radars, cross-eye jamming is used etc [12].

Passive ECM does not make use of electromagnetic energy; rather, it employs confusion reflectors for the deception of enemy's electronic system. This is achieved by chemical or mechanical means.

- **Chemical Jamming**: It involves the use of smoke and chemical agent like aerosols to deceive the enemy [10].
- **Mechanical Jamming**: This involves deception of enemy's electronic warfare aids by the use of specially designed mechanical objects like chaff, flares, drones etc.

Chaff is an electronic equivalent of smoke. Instead of scattering or absorbing electromagnetic energy, as in the case of smoke, it reflects electromagnetic energy in order to confuse an enemy electronic system. Chaff consists of thin metal-coated dielectric fibers. It forms a cloud of metallic dipoles and appears on the enemy's radar screens as a blot, thereby masking the real target signal [17]. A flare is a pyrotechnic target launched from an aircraft causing infrared (IR) missiles and other optical devices to be decoyed away from the true target. The flares are dispersed when the heat-seeking missile approaches its target to divert them from the target [13]. Decoys like remotely piloted vehicles (RPVs), drones, and other aircraft-type vehicles are also some other means of deception. The objective of decoys is to trigger the enemy's radar so as to force them to reveal their presence, location, and operating characteristics. This information is very useful for the forces which are trying to counter such a radar threat [10].

### 3) ELECTRONIC PROTECTION (EP)

EP, also known as Electronic Counter-Counter Measures (ECCM), ensures friendly, effective use of the electromagnetic spectrum despite the enemy's use of EW. The fundamental difference between ECCM and ECM is that ECM involves techniques to provide jamming and decoy methods, whereas ECCM is concerned with techniques that are embodied in the design of electronic equipment (e.g., radar and its constituent parts like receiver, transmitter, etc.) to overcome these methods. Most of the ECCM techniques are based on the characteristics of radar parameters like power, frequency, PRF, pulse length, antenna gain, antenna polarisation, receiver's probability of intercept, etc [14]. Some commonly used ECCM techniques in terms of spatial, spectral, temporal, and netting domains are shown in Figure 2.

- **Spatial ECCM**: This category of ECCM includes methods which are space based. Some of the methods under this category are as follows [13], [17]:
  - **Side lobe canceller**: This technique is used on surveillance or tracking radar. This method prevents the noise jamming signal from adversely affecting the radar's operation. All false signals entering the side lobe of the main antenna get cancelled at the output.
  - **Side lobe blanking**: This device employs an auxiliary wide-angle antenna and receiver to determine whether a received pulse is from the side lobe region. If signal from the side lobe region of antenna is detected then it is blanked from the output signal.
  - **Burn through technique**: This method enables the appearance of a true target on a radar indicator even in a jamming environment. In this technique, radar increases its energy on the target in order to illuminate the targets in a jamming environment
- **Spectral ECCM**: This category of ECCM includes methods which are frequency based. Some of the methods under this category as discussed in, [17], and [18] are:
  - **Low probability of intercept (LPI) technique**: This technique attempts to escape detection by an intercept receiver. This is attained by using

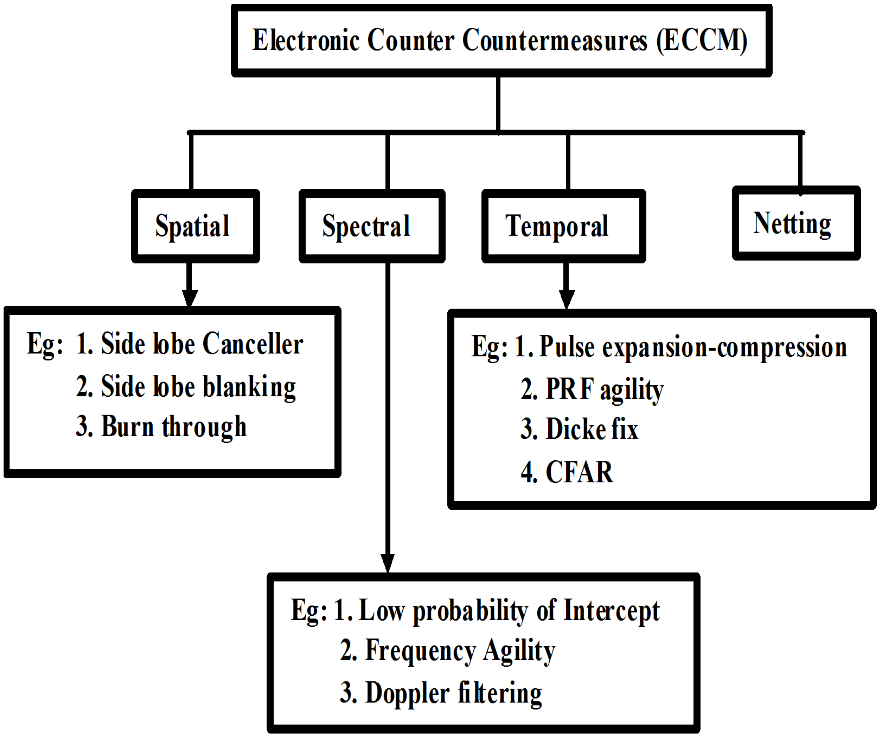

**FIGURE 2.** ECCM Techniques.

antenna having low side lobes and spread spectrum transmissions.

- **Frequency agility**: This is another ECCM technique which is use to counter the jamming signal. This technique enables the radar to rapidly change its transmitter and receiver operating frequency, sometimes on a pulse-to-pulse basis.
- **Doppler filtering**: This technique is used on a tracking doppler radar. Doppler radar is a specialized radar that uses the Doppler effect to produce velocity information about the target. The objective of this method is to detect doppler targets and to aid in defeating velocity deception techniques.

- **Temporal ECCM**: This category of ECCM includes techniques which are time-dependant. Some of the methods under this category are as follows [14], [18]:
  - **Pulse expansion-compression**: This technique is used to counter some types of noise jamming and deception jamming. A pulse signal is expanded for transmission. This expanded pulse is transmitted and decoded on its return. In the decoding process, Echo responses are then compressed. This provides longer detection ranges and wideband short pulse, thereby increasing the target range resolution.
  - **PRF agility**: This is an anti-interference technique that is used on tracking pulse radar to degrade the effectiveness of a pseudo target repeater. In this technique, PRF is rapidly varied at a random rate so that the pseudo targets appear fuzzy on the radar scope. This method helps to increase the radar's capability in a dense signal environment.
  - **Dickefix**: This technique is used to counter wideband sweep jamming and other related ECM techniques, which uses a wideband IF amplifier and a limiter ahead of the normal bandwidth IF amplifier in the radar receiver.
  - **Constant false alarm rate (CFAR)**: This technique is used for prevention of radar receiver saturation, and overload [10]. It allows the radar to function properly in an environment where interference due to signals from jammers and other radiating sources are present. The presence of these interfering signals in radar with automatic threshold detection can increase the rate of false alarms to an intolerable extent. When the radar output data is processed in a computer, the device might be overloaded by the added false alarms due to jamming. So, this CFAR technique keeps the detection of false alarm rate constant when the radar is receiving these interfering signals [15]. However, detection of a target is not possible in this method if the target is weaker than the jammer, but an ambiguous situation due to the presence of jammer can be removed.

- **Radar Netting**: Radar net is a combination of at least two or three radars that feeds information to a central hub from where the commander directs the conflicts in the

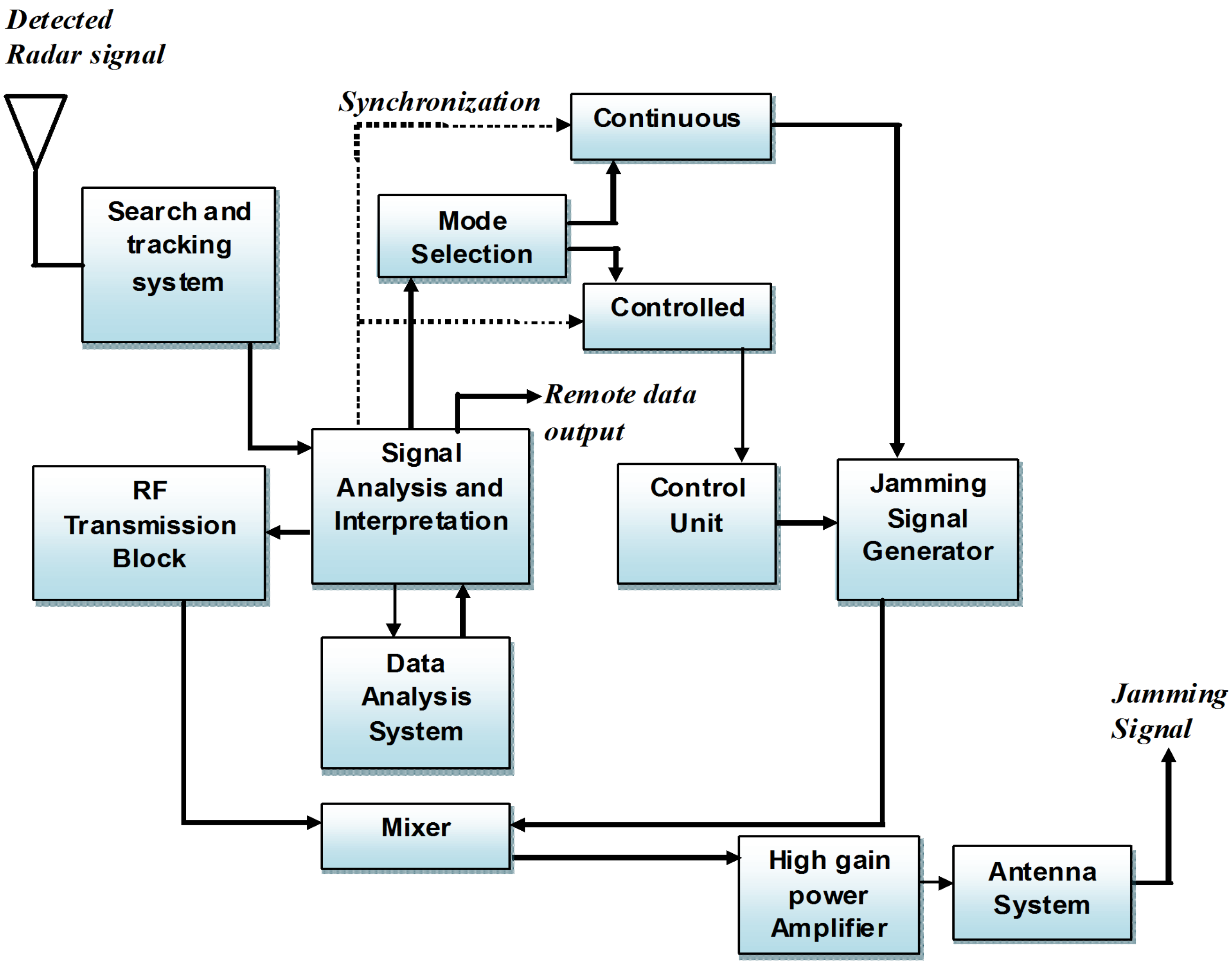

FIGURE 3. Block diagram of a typical EW system.

battlefield. This technique increases the potential ECCM capability of the system.

A typical block diagram of EW system for disruption in radar based detector and surveillance system is shown in Figure 3. It is certainly not the only configuration available for EW systems, the design of such systems depends on a particular application.

The function of search and tracking system is to determine the location or direction of a target on a continuous basis. Search and tracking system basically consist of receivers which cover a number of specific radar bands. This receiver identifies the frequency of the transmitted signal, AOA of the signal in order to calculate the location of the transmitter. Signal analysis and interpretation unit comprise of a frequency counter, spectrum analyzer and a video display unit [14]. It measures the values of signal parameters like PRF, pulse width, polarisation, amplitude, etc., present in the received signal. This information can also be feed to a remote data system. The remote data system is a tactical indicator to display threat category, frequency of transmission, and signal parameters. Data from the signal analysis and interpretation unit is fed to the data analysis system for threat evaluation and storage purposes. RF transmission block consists of a signal processor, pulse code modulation (PCM) encoder, pre-modulator, and RF transmitter. The function of this module to process the analog signals coming from the signal analysis and interpretation unit and converts them to a digital form for application in the modulation circuits of a radio communication transmitter. The jamming signal generator is made up of wideband and spot tuning microwave circuits. Jammer prevents threat radar from measuring target position and velocity. It transmits RF noise signals like amplitude modulated (AM) or frequency modulated (FM) signal into the enemy's electronic system so as to completely masked the target signal. The modulation can take many forms, depending on the target signal, but random noise is commonly used for communication signals. Data from the signal analysis and interpretation module also goes to a mode selector. There are two modes in the mode selector, namely continuous and control mode. In continuous mode, the system generates the jamming signal continuously, and in controlled mode, the jamming action is determined by the control unit. The Control unit supervises the passage of data from the signal analysis and interpretation module to the jamming signal generator module. For jamming techniques, where the jammer works in the repeater mode without performing any analysis, in those circumstances control unit blocks the passage of data from the signal analysis and interpretation unit to the jamming signal generator unit. Finally, the jamming signal is mixed with a RF signal and passed through a high-power amplifier. A high gain power amplifier amplifies the signal from the jammer. Jammer antenna system directs the jamming signal to the target. A special jammer receiver, along with a servo system, keeps the antenna aligned on the selected target.

### B. AI FUNDAMENTALS AND RELEVANT TECHNIQUES

AI is defined as non-human intelligence that is used to develop a computer system in such a manner that it can replicate human mental skills. The commonly used AI techniques are Machine Learning (ML), including Artificial Neural Network (ANN) and Deep Learning (DL) or Deep Neural Network (DNN), Fuzzy Logic, Genetic algorithm, etc. These techniques are briefly discussed below.

#### 1) MACHINE LEARNING

- **Artificial Neural Network (ANN)**: An ANN is a non-parametric computational tool that can be trained to perform various computational tasks like pattern recognition, classification, data clustering, etc. The basic computation unit in an ANN is the artificial neuron, which can generate outputs after receiving inputs replicating the biological counterpart. These neurons are interconnected by links (synapses) with weights and are grouped in layers to form a network designed to process an input signal. The network has an input layer, any number of hidden layers, and an output layer. ANNs may have two different types of network topology, namely feedforward and feedback network. A Feedforward network is a non-recurrent network, and information flow is unidirectional. A feedback network is a recurrent network where information can flow in both directions using loops. The learning mechanism used in ANNs may be supervised or unsupervised learning. Multi layer perceptron (MLP) is the simplest feedforward ANN trained with a back-propagation algorithm. It is a non-parametric learning-based technique best suitable for prediction, classification, and regression. Another example of feedforward ANN is the time delay neural network (TDNN). Recurrent neural network (RNN) and nonlinear autoregressive network with exogenous inputs (NARX) are examples of feedback ANN. MLP doesn't have time processing capability, whereas TDNN, RNN, and NARX demonstrate the ability to process time dependent signals. The basic mathematical steps of each of these methods are mentioned below:

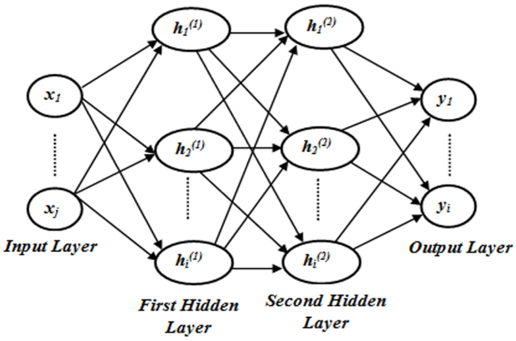

**FIGURE 4.** MLP with two hidden layers.

  - **MLP:** A MLP with two hidden layer is shown in Figure 4. It is a fully connected network, so every unit receives connections from all the units in the previous layer. Each unit has its own bias and there is a weight for every pair of units in two consecutive layers [19]. Let '$x_j$' be the input units, 'y' be the output unit, units in the $l^{th}$ hidden layer be denoted as $h_i^{(l)}$. The network's computations are shown in equation 1-3.

$$h_i^{(1)} = \psi^{(1)}(\sum_j w_{ij}^{(1)} x_j + b_i^{(1)}) \tag{1}$$

$$h_i^{(2)} = \psi^{(2)}(\sum_j w_{ij}^{(2)} h_j^{(1)} + b_i^{(2)}) \tag{2}$$

$$y_i = \psi^{(3)}(\sum_j w_{ij}^{(3)} h_j^{(2)} + b_i^{(3)}) \tag{3}$$

where, $\psi$ is the activation functions, $w_{ij}$ is the respective weights, $b_i$ is the bias. These equations can be written in vector form as shown in equation 4-6

$$h^{(1)} = \psi^{(1)}(W^{(1)}x + b^{(1)}) \tag{4}$$

$$h^{(2)} = \psi^{(2)}(W^{(2)}h^{(1)} + b^{(2)}) \tag{5}$$

$$y = \psi^{(3)}(W^{(3)}h^{(2)} + b^{(3)}) \tag{6}$$

where, $h^{(l)}$ is the activation vector, that represents the activations of all units, $W^{(l)}$ is the weight matrix, that represent weights of each layer, $b^{(l)}$ is the bias vector. By combining all the training examples into a single matrix 'X', the computations in matrix form can be written as shown in equation 7-9.

$$H^{(1)} = \psi^{(1)}(XW^{(1)T} + b^{(1)T}) \tag{7}$$

$$H^{(2)} = \psi^{(2)}(H^{(1)}W^{(2)T} + b^{(2)T}) \tag{8}$$

$$Y = \psi^{(3)}(H^{(2)}W^{(3)T} + b^{(3)T}) \tag{9}$$

where, $H^{(l)}$ is a matrix that stores hidden units of each layer for all the training examples. Training of MLP networks is done using back-propagation algorithm. In this algorithm a set of training samples are presented to the network and network computes the output. Since the connection weights in the network starts with random values, after the first iteration the calculated output does not match the desired output. Hence, the network needs some form of error correction. The mean square error function is defined by equation 10

$$E(w) = \frac{1}{2N}\sum_{n=1}^{N}(y_i - y_t)_n^2 \tag{10}$$

where 'N' is the number of training samples. MLP's training is implemented by updating the weight vector '$w$' in order to minimize the mean square error 'E($w$)'. The weights are updated using equation 11 [19].

$$w(n+1) = w(n) - \eta\frac{\delta E}{\delta w(n)} \tag{11}$$

where '$w(n$+1)' is the new weight, '$w(n)$' is the previous weight and '$\eta$' is the learning rate.

- **RNN:** It is a type of ANN that contains loops, allowing information to be stored within the network. RNN can perform any nonlinear mapping like MLP, but the difference is that the response to an input from a recurrent network is based on all previous inputs, as these are used in feedback connections. Due to feedback connections, the recurrent networks can obtain state representations, thereby becomes suitable devices for different dynamic applications. Each computation layer of an RNN has feedback around it, as shown in Figure 5 for the case of RNN with two hidden layers. Let '$x_1(n)$' denotes the output of the first hidden layer,'$x_2(n)$' denotes the output of the second hidden layer and so on. Let '$y_0(n)$' denotes the output of the output layer. Then the dynamic behaviour of the RNN, in general, in response to an input vector '$u(n)$' is described by the following equations [19]:

$$x_1(n+1) = \psi_1(x_1(n), u(n)) \tag{12}$$
$$x_2(n+1) = \psi_2(x_2(n), x_1(n+1)) \tag{13}$$
$$y_0(n+1) = \psi_0(y_0(n), x_k(n+1)) \tag{14}$$

where, $\psi_1(.)$, $\psi_2(.)$,$\psi_0(.)$ denotes the activation functions characterizing the first hidden layer, second hidden layer and output layer of the RNN respectively and 'k' denotes the number of hidden layer in the network. Training of an RNN is done by using a back-propagation through time (BPTT) algorithm.

- **NARX:** It is a recurrent dynamic neural network consisting of several layers with feedback connections from output to input [20]. There are two types of input in a NARX network: the exogenous and previous output of the network. In the case of non-linear time series prediction, NARX neural network utilizes its memory ability to remember the past values of predicted time series. This network can have two architectures: series-parallel (open loop) and parallel (closed-loop), as shown in Figure 6. The behaviour of this network, in general, is described by equation 15 and 16 [20]

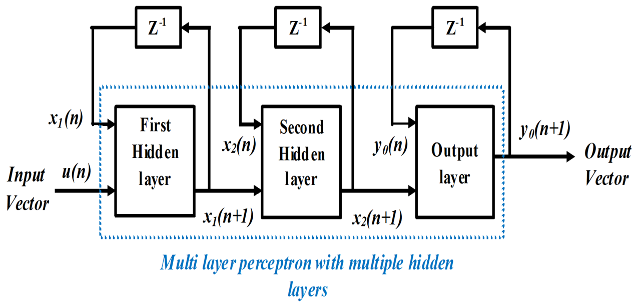

**FIGURE 5.** RNN with two hidden layer.

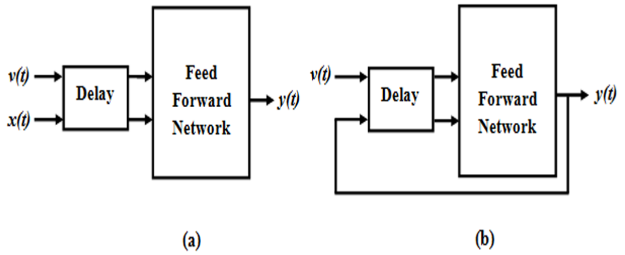

**FIGURE 6.** NARX architecture: (a) Series-parallel architecture (b) Parallel architecture.

**(a)** For series-parallel architecture:

$$\begin{aligned} y(t) &= f(x(t-1), x(t-2), \ldots., x(t-n_x), \\ &\quad v(t), v(t-1), v(t-2), \ldots, v(t-n_v)) \end{aligned} \tag{15}$$

**(b)** For parallel architecture:

$$\begin{aligned} y(t) &= f(y(t-1), y(t-2), \ldots., y(t-n_x), \\ &\quad v(t), v(t-1), v(t-2), \ldots, v(t-n_v)) \end{aligned} \tag{16}$$

where, '$f(.)$' is the mapping function, '$y(t)$' is predicted output of the system at time 't', '$v(t)$' is current input, $x(t-1), x(t-2), \ldots., x(t-n_x)$ are the original past outputs, $y(t-1), y(t-2), \ldots., y(t-n_x)$ are the predicted past outputs, $v(t-1), v(t-2), \ldots, v(t-n_v)$ are the past inputs and '$n_x$' and '$n_v$' are the number of output and input delays respectively.

- **TDNN:** It is a multi-layer, feed-forward network whose hidden neurons and output neurons are replicated across time. TDNN is made up of units that

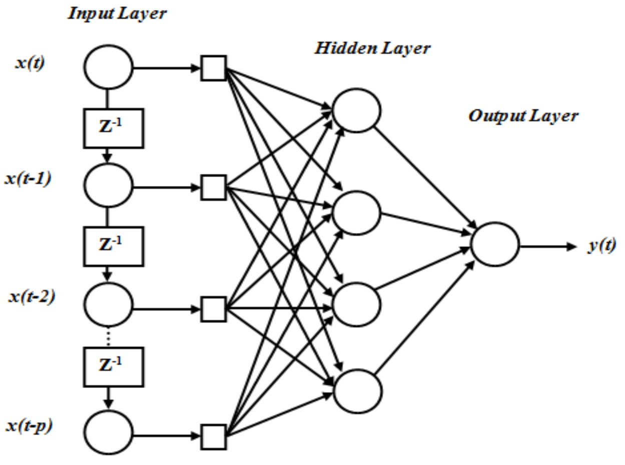

**FIGURE 7.** Architecture of TDNN.

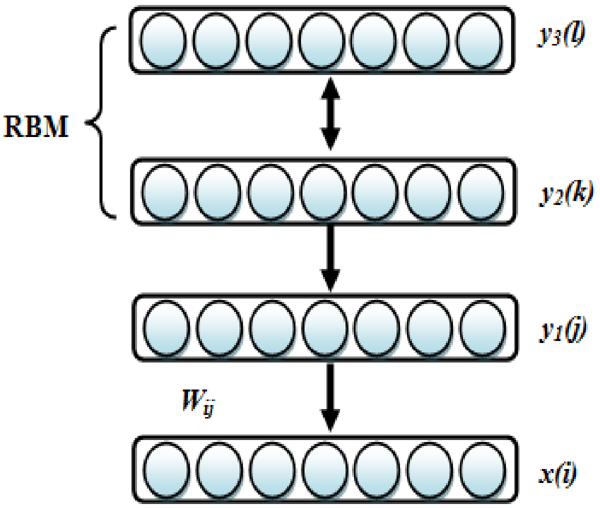

**FIGURE 8.** Deep belief network structure with three hidden layers.

get input at the generic time instant 't' and an output of the previous level units, in which the input at several time steps t-1, t-2,....t-p is summed and fully connected with suitable weights. These delayed inputs provide part of the signal's history at the time 't' and enable the solution to more complex decision problems, especially time dependent ones. A simple architecture of a TDNN is shown in Figure 7. The layout of the TDNN includes an input layer, one or more hidden layers, and an output layer. Additionally, the network input layer utilizes the delay components embedded between the amounts of input-units to attain the time-delay [21]. The input-output relationship is given by $y = f(x(t), x(t-1), \ldots., x(t-p))$. Consequentially, the TDNN is to seek the relationship function '$f$' of the input-output in the network. This is given by $h_j = \phi(\sum_{l=0}^{p} w_{ij} \times x(n-l) + b_j)$ and $y(n) = \phi(\sum_{j} w_{jk} h_j)$, where $h_j$ and y(n) are the function at the hidden and output layers, respectively; p is the number of tapped delay nodes; $W_{ij}$ is the weight of the $i^{th}$ neurons in the input layer into the $j^{th}$ neurons in the hidden layer; and $b_j$ is the bias of the $j^{th}$ neurons. The function $\phi(.)$ represents a nonlinear sigmoid function. Training of the TDNN takes place through back-propagation algorithm.

Other commonly used supervised learning-based techniques are naive bayes, support vector machines (SVM) and random forests, etc [22]. ANN-based AI techniques find its application in different categories of EW domain [23]–[30]. Some example from the literature includes emitter signal identification and classification, recognition of radar antenna scan parameter, for suitable jamming style selection, etc.

- **Deep Neural network (DNN)**: As compared to neural networks, DNN has better feature expression and ability to fit the complex mapping [31]. DNN extracts feature layer by layer, thereby combine low-level features to form high-level features. There are three commonly used DNN model, namely Deep Belief Networks(DBN), Stacked Autoencoder (SAE), Deep Convolution Neural networks (DCNN) [32].
  - **Deep Belief Network (DBN)**: It is an Unsupervised Probabilistic Deep learning algorithm. DBNs are composed of layers of Restricted Boltzmann Machines (RBMs) for the pre-train phase and then a feed-forward network for the fine-tune phase. An RBM is an undirected energy based model with two layers of visible (x) and hidden (y) units, respectively, and have connections only between layers. The RBM algorithm is useful for dimensionality reduction, classification, regression, feature learning, etc. The restriction in a RBM is that there is no intra-layer communication. Generally, a DBN is formed by an arbitrary number of RBMs stack on top of each other. This gives a combination between a partially directed and partially undirected graphical model [33]. An example of DBN with three hidden layers is shown in Figure 8. Therefore, the joint distribution between visible layer 'x' i.e. input vector and the 'n' hidden layers '$y^k$' is defined by equation 17.

$$p(x, y^1, \ldots., y^k) = \prod_{k=0}^{n-2} P(y^k | y^{k+1}) P(y^{n-1}, y^n) \tag{17}$$

where, $P(y^k|y^{k+1})$ is a conditional distribution for the visible units conditioned on the hidden units of the RBM at level k, and $P(y^{n-1}, y^n)$ is the visible-hidden joint distribution in the top-level

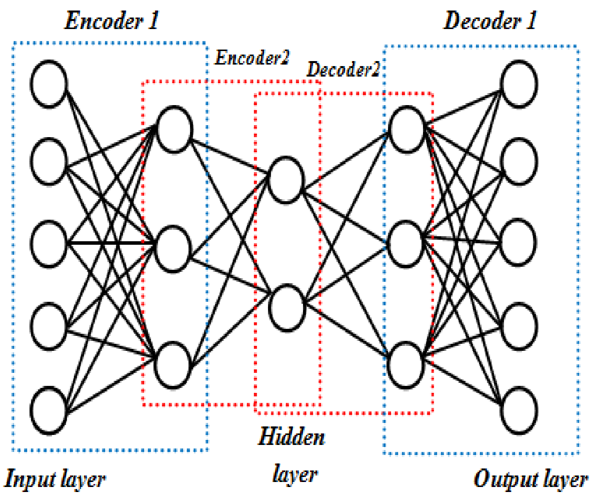

**FIGURE 9.** Architecture of Stacked Autoencoder.

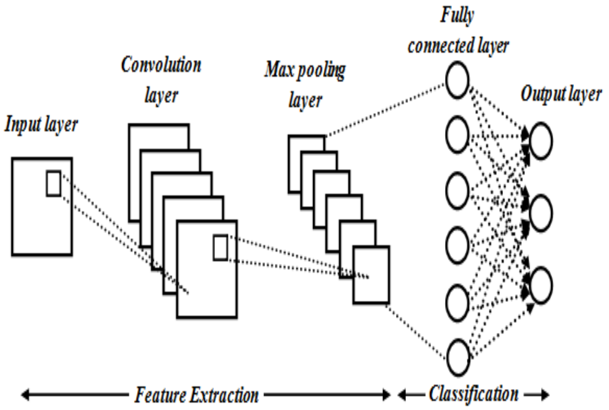

**FIGURE 10.** Architecture of DCNN.

RBM. The principle of greedy layer-wise unsupervised training can be applied to DBNs. This is done by training each RBM separately from it, in a bottom to top fashion, and using the hidden layer as an input layer for the next RBM.

- **Stacked Autoencoder (SAE)**: It is an unsupervised learning based neural network. In SAE, autoencoder is used [34].The process of training in this method consists of two parts: encoder and decoder. Encoder is used for mapping the input data into hidden representation whereas decoder reconstructs input data from the hidden representation [35]. The structure of SAE is formed by stacking '$k$' autoencoders into '$k$' hidden layers.Then an unsupervised layer-wise learning algorithm is used, followed by fine-tuning with a supervised method. The architecture of an stacked autoencoder is shown in Figure 9. Given the unlabeled input dataset '*x(n)*', the encoding process is defined by equation 18 [36].

$$h_n = \phi(w_1 x_n + b_1) \tag{18}$$

where, $h_n$ represents the hidden encoder vector calculated from *x(n)*. $\phi(.)$ is the encoding function, $w_1$ is the weight matrix of the encoder, and $b_1$ is the bias vector. The decoding process is defined by equation 19 [36].

$$y_n = \psi(w_2 h_n + b_2) \tag{19}$$

where, $y_n$ is the decoder vector of the output layer, $\psi(.)$ is the decoding function, $w_2$ is the weight matrix of the decoder, and $b_2$ is the bias vector.

- **Deep Convolution Neural network (DCNN)**: It represents feed-forward neural networks that comprise various combinations of the convolutional layers, max-pooling layers, and a fully connected neural network. It exploits spatially local correlation by enforcing a regional connectivity pattern between neurons of adjacent layers [35]. The structure of DCNN is shown in Figure 10. The convolution layers create feature maps by convolving kernels over feature maps in layers below them. The max-pooling layers downsample the feature maps by a constant factor [37]. The activations $x_j^l$ of a single feature map j in a convolution layer l is given by equation 20:

$$x_j^l = f(b_j^l + \sum_{i \in M_j^l} x_i^{l-1} * w_{ij}^l) \tag{20}$$

where, *f(.)* is a non-linear function, typically tanh() or sigm(), $b_j^l$ is a scalar bias, $M_j^l$ is a vector of indexes of the feature maps $i$ in layer $l$ - $1$ which feature map $j$ in layer $l$ should sum over, $*$ is the 2 dimensional convolution operator and $w_{ij}^l$ is the kernel used on feature map $i$ in layer $l$ - $1$ to produce input to the sum in feature map $j$ in layer $l$. For a single feature map $j$ in a max pooling layer $l$, the activation is defined as shown in equation 21.

$$x_j^l = down(x_j^{l-1}, N^l) \tag{21}$$

where, down is a function that down samples by a factor $N^l$. Finally, for classification purpose, a fully connected output layer is used which is denoted by equation 22. It takes the concatenated feature maps of the layers as an input.

$$y = \phi(w^0 f_v + b^0) \tag{22}$$

where $b^0$ is a bias vector and $w^0$ is a weight matrix, $f_v$ is the concatenated feature vector and $\phi(.)$ is the nonlinear activation function.

Deep learning plays a significant role in EW systems for radar signal processing, emitter identification and classification, developing improved anti-jamming methods, detection of jammer and its characteristics, etc. A few related works are presented in [8], [9], [28], [38]–[40], [41], [42], [43].

### 2) FUZZY SYSTEMS

Fuzzy Logic combines traditional crisp set with statistical grading performed by membership functions enabling it to track finite variations in inputs. Fuzzy systems attempt to resemble the human decision-making methodology using ANN and deals with vague and imprecise information [44]. Fuzzy systems have no learning capability or memory. Hence, fuzzy modelling is often combined with other techniques to form hybrid systems, e.g., neuro-fuzzy systems, which is a combination of neural network and fuzzy system. These have been widely used in a host of radar and related signal processing applications [45].

### 3) GENETIC ALGORITHM (GAs)

GA attempts to replicate the naturally occurring evolution processes, supporting survival of the fittest while deriving an optimal solution. It is an iterative technique based on probability. The algorithm progresses until it satisfactorily solves the problem. The fitter solutions in a population survive and pass their traits to offspring, which replace the poorer solutions. Unlike some random search techniques, which give a single solution, GA keeps a pool of solutions, thereby reduces the probability of reaching a false optimum [44]. GA has been preferred for a range of optimization problems. These have been combined with ANN and DNN for several dynamic environments [46]. Similarly, fuzzy systems have been combined with GA and applied in a range of applications including radar signal processing [45].

In the subsequent sections, the authors enumerate the importance of AI in EW and highlight a few specific applications.

## III. ROLE OF AI IN EW

The importance of EW has gradually grown as modern military command and control has emphasized connectivity through all echelons [47]. AI enabled EW systems are reconstructing the fundamental nature of military technologies [48]. Inclusion of AI algorithm in an EW system makes them highly effective as autonomous systems. EW systems of all modern militaries are heavily reliant on autonomous algorithms [47]. With the increasing demand of automation of EW systems, modern AI algorithms are being investigated to determine their value as an addition to upcoming EW systems. AI can be used in diverse domains of military activity like weapons systems selection and employment, decision support, threat analysis, interpretation of intelligence, logistics etc. For military applications, AI supported data processing systems are already in use and intelligent communication attributes have become indispensable [7], [8], [24], [25], [49]. These applications tend to fall into two categories: AI based EW systems that affect the operational level of war and those that affect the strategic level. At the strategic level, application of AI could affect how the military department organize the order of battle, assignments to forces, war strategies, decisions about the scale and escalation, intelligence sharing and interpretation, scope and nature of war, consequence of deployment of specific assets etc. Application of AI at the operational level of battle could have a very significant influence in achieving tactical objectives, planning, removing uncertainty and effective preparedness. Some of these aspects are discussed below:

- **Application of AI at operational level of war**: Some examples of application of AI at the operational level of war are discussed below:
    1) AI in information collection, interpretation and analysis: In military arena, information are collected from signal intelligence (SIGINT), ELINT, human intelligence (HUMINT), measurement and signature intelligence (MASINT) etc. All these information need proper interpretation and analysis to make them useful for decision making. The issues of information overload faced by the intelligence community is sought to be effectively handled by using machine learning [50]. This will help all the source analysts to understand an evolving security environment. In this respect, an AI enabled system can be useful for strategic stability.
    2) AI in war gaming: AI can increase the power of simulations and gaming tool that is used to study the battle field scenario and conventional weapons. AI can enable planners to model battle field scenario in order to explore how dynamic conditions may affect outcomes and decision making and can also be used to analyze the results of such scenario.
    3) AI in unmanned vehicle: AI based navigation software enables UAV to find their way through hostile territory. AI equipped drones can conduct advanced battle tactics and immediately adjust to enemy war games to exploit battle field opportunities. When combined with robots, AI can increase the ability of machines to operate autonomously [51].
- **Application of AI at strategic level of war**: Some examples of application of AI at the strategic level of war are discussed below:
    1) AI in Intelligence, Surveillance and Reconnaissance (ISR): AI can play a very significant role in processing the information of military importance. ISR is very important for multi domain situational awareness. AI can be a very significant tool in managing this huge amount of ISR data involved in modern warfare. AI can be useful in analyzing the real time dynamic battle field conditions. Moreover, AI can also make it possible to attack quickly and optimally while minimizing the risks to one's own forces.
    2) AI enable advance targeting and navigation techniques can have improved prospects for a wide

range of tactical and strategic defence system by allowing target acquisition, tracking and discrimination [50].

3) AI guided probing, mapping and hacking of computer networks can provide useful information for both offensive and defensive purpose [50].

The AI techniques can also be used in signal intelligence systems to detect RF signals intercepted from opponents and predict the threats [52]. It can help in decoding RF signals sent out by communications or radar systems. Convolutional neural network (CNN) can be used for improving DOA estimates for EW systems [9]. Based on images created by time-frequency images of the radar signals DNN can be used to classify radar pulses [38]. Competitive deep reinforcement learning-based methods can be used in ECCM system for adapting ones' own communications to an EW environment where the adversary is using adaptive jamming [39]. Current trends of application of AI based techniques in radar signal processing and EW from state of the art is briefly discussed in the following subsection.

### A. REVIEW OF CURRENT TRENDS OF APPLICATION OF AI BASED TECHNIQUES IN RADAR SIGNAL PROCESSING AND EW

Various AI algorithms that can be used as part of EW techniques include range of neuro-computing and deep learning techniques which acquire knowledge from the surroundings, retain it and use it subsequently.

The method discussed in [5] shows the analysis of data sets gathered through electronic warfare for determining regions where target elements are concentrated through application of density based special clustering (DBSCAN) and K-Means algorithms. In [49], a method on radar visual range of electronic warfare simulation based on transcendental equation method and graphic space intersection method is discussed. A Novel learning algorithms based on the multi-armed bandit framework is discussed in [6] to optimally jam malicious transmitter-receiver pairs in an electronic warfare-type scenario without having any apriori knowledge about the system. A soft-computing based model to realize an autonomous decision-making process for threat detection, classification, and the selection of alternative counter measures against threats in EW settings is discussed in [7]. In [45], AI techniques i.e. fuzzy logic and neural networks, for decision making in EW environment based on influential parameters for the specific scenario is discussed. A novel delayed learning framework with transition-based rewards is discussed in [23]. For an ESM, it is essential to recognize the modulation of pulse repetition intervals (PRIs), to extract information about the radar emitters. PRI modulations are difficult to recognize in modern electronic environments due to a large number of spurious pulses. An automatic method for recognizing seven PRI modulation types using a CNN is discussed in [8].Another improved algorithm for PRI modulation recognition is discussed in [24]. This method can recognize four different PRI modulation types using a three- layer neural network. A radar signal intra-pulse modulation recognition method based on convolutional de-noising autoencoder (CDAE) and deep convolutional neural network (DCNN) is discussed in [38]. In this method, at first radar signals are converted into time-frequency images (TFIs). These images are then pre-processed using bilinear interpolation and amplitude normalization method. CDAE is then used to denoise and repair TFIs. A DCNN based on Inception architecture is then designed to identify the processed TFIs. Similarly, an automatic modulation classification system for radar signals based on hybrid AI based algorithm including naive Bayesian and SVM is presented in [53]. In this method, the modulation features of the radar signal is extracted using a set of algorithms that comprises of time-frequency analysis, discrete Fourier transform, and instantaneous autocorrelation. This method can successfully classify seven types of signal in different modulation type namely binary phase shift keying (BPSK), quadrature phase shift keying( QPSK), 16-quadrature amplitude modulation (16QAM), linear frequency modulation (LFM), single frequency (SF), 2FSK, and 4FSK. The performance of a deep reinforcement learning (DRL)-based anti-jamming method is discussed in [39]. At first an intelligent jamming method based on reinforcement learning is designed to combat the DRL-based user. Then, the conditions when the DRL-based anti-jamming algorithm cannot converge are theoretically analyzed. Thereafter, various scenarios where users with different communicating modes combat jammer with different jamming modes are compared in order to investigate the performance of DRL-based method. A method based on deep learning is proposed in [9] to select antennas in a cognitive radar scenario. A DNN is constructed with convolutional layers as a multi-class classification framework. The training data is generated such that each class indicated an antenna subarray. These results in lowest minimal error bound for estimating target DOA in a given scenario. Wireless networks are prone to jamming attacks. The transmission performance further deteriorates when the jammer focus their signals on reference signals of the transmitters. The AI based method presented in [40] is capable of jointly determining the presence of the jammer, along with its attack characteristics. The presence of the jammer is determined by using two different neural networks namely DCNN and deep RNN. The presence of jammer and its type is determined through a diverse set of scenarios that are implemented on software defined radios.

With the rapid development of EW systems, there arises the need of proper electromagnetic environment observation in order to analyze target radar signatures. MASINT plays a significant role in this direction [54]. MASINT helps to detect, track, identify and describe the distinguishing characteristics of emitters. These distinguishing characteristics of radio electronic devices are the important element in the process of recognition and identification of the emitter [54]. In advanced systems, analysis and processing of these distinctive features for recognition and identification of emitter involves the procedures like analysis of signal parameters measured in a dense electromagnetic environment, automatic emitter sources identification by comparing signal parameters from a database as early as possible, use of specific expert's knowledge in the process of identification and location of emitters for detection of unknown signals. Moreover, it also involves methods of pulses de-interleaving in case of simultaneous signal from many emitters and updating mechanism of the database. In this direction, a method of specific emitter identification based on graphical representation of the distribution of radar signal parameters is presented in [54]. This method is based on transformation and analysis of distribution of basic radar parameters especially Pulse Repetition Interval.

A system for radar signal recognition based on non-negative matrix factorization network (NMFN) and ensemble learning is presented in [41]. This system can recognize nine different radar signals even at the condition of low signal to-noise ratio (SNR). At first, a feature extraction algorithm based on pre-trained convolutional neural network (CNN) is developed. Then based on the theory of network, NMFN is developed to extract features and to reduce the redundant information. Thereafter to further improve the performance of recognition rate, feature fusion algorithm based on SAE is developed to get the more essential expression of feature. Finally, improved artificial bee colony (IABC) algorithm is presented as the scheme of ensemble learning which combine three classifiers together to get more accurate recognition results.

A novel method for radar emitter signal identification and classification based on Ward's clustering and probabilistic neural networks (PNN) is discussed in [25]. Initially, self-adaptive filtering and Fourier transform are used to obtain the frequency spectrum of the signals. Then the range of the optimal number of clusters is obtained by using the Ward clustering method and some clustering validity indexes. The PNN is used as a classifier in this method.

In [26], ANN based method for timely and reliable recognition of radar signal emitters is presented. The method involves a large data set of intercepted generic radar signal samples for investigating and evaluating several ANN topologies. Three case studies are discussed in [26] and several data coding, data transformation and learning parameters are evaluated. An automatic radar waveform recognition system to detect, track and locate the low probability of intercept (LPI) radars is discussed in [55]. The system can classify 12 different types of pulse wave radar signals with a low signal-to-noise ratio (SNR). The method uses a hybrid classifier which includes two relatively independent subsidiary networks namely convolutional neural network (CNN) and Elman neural network (ENN).

Another neural network based radar signal classification system is presented in [27]. This method introduces a novel feature extraction algorithm based on probability moment and approximate entropy (ApEn) for radar signal classification. The antenna acts as a radiation device for radar signal and its characteristics determines the performance of the radar. In order to determine the target, the radar antenna beam required to be search in a certain manner, which corresponds to a parameter known as antenna scan type. The accurate recognition of antenna scan type of hostile radar is important for the threat assessment. In this direction, a method combining the Visibility graph with machine learning for recognition of radar antenna scan pattern is discussed in [28]. At first, seven radar antenna scan patterns are modelled. Then the time series of the scan patterns are converted into a visibility graph and the visibility graph feature extraction is performed. Thereafter, the extracted six types of features are sent to the classifier for identification of the signals. The support vector machine (SVM), back propagation (BP) neural network, naive Bayes algorithm, MLP and DBN is used as a classifier in this method. Another algorithm for estimation of the radar antenna scan period (ASP) and recognition of the radar antenna scan type in EW environment is presented in [29]. This method involves scan period estimation followed by pre-processing using normalization, re-sampling and averaging techniques, feature extraction, and classification. Naive Bayes (NB), decision-tree (DT), ANN, and SVM classifiers are used to classify five different antenna scan types Since ESM receivers are required to carry out high amount of computations in real-time, technique like compressive sensing (CS) can be very useful for reducing the computational cost of such receivers [42]. CS-based EW receivers are able to detect and locate targets using only a small number of compressively obtained samples in much less computational cost compared to the traditional EW receivers. One such CS based ESM receiver design is presented in [42] to estimate the angle-Doppler of adversary targets whose waveforms are not known. The receiver uses a Sparse Bayesian Learning (SBL) framework, which is blind in the sense that the knowledge of the sparsity basis is not available. An innovative framework for testing various CEW tasks, in which the DRL algorithm has been used for the target searching purpose, is discussed in [43]. This method depicts how to overcome, the spatial sparsity, continuous action, and partially observable environment that exist in cognitive EW that can limit the abilities of DRL algorithms. To realize this task Python is used to build a 3-D space game Explorer to simulate various cognitive EW environments in which the electronic attacker is an unmanned combat air vehicle (UCAV) and the defender is an observation station.

The chaotic compound short-range detection system is a system that has strong anti-jamming ability [46]. For the deception jamming case, the features of the complex short-range detection system are close to the echo detection. This causes a serious threat to the detection system. In this direction, a technique that can extract and analyze different features of deceptive jamming and target echo signal in order to realize the anti deceptive jamming of chaotic compound short-range detection system is discussed in [46]. The method simulates the mathematical model of deceptive jamming and target echo. Thereafter analyzes the bi-spectral characteristics of the simulated echo and jamming signal.

A set of anti-deception jamming feature parameters is then constructed. The task of identification of deceptive interference is accomplished by GA-back propagation neural network technique. A jamming style selection method based on jamming rule base is described in [30].The radar signal parameter like PRF, pulse width, pulse amplitude, angle of arrival etc are used for construction of jamming rule base. This method can play a significant role in improving the accuracy and real-time performance of the cognitive EW intelligence countermeasure system.

Different types of jamming signals interferes the radar in detection, tracking, and targets reorganization operations. The filtering method based on stacked bidirectional gated recurrent unit network (SBiGRU) and infinite training is discussed in [56]. This method tends to suppress the Interrupted-sampling repeater jamming (ISRJ) signal for pulse compression (PC) radar with linear frequency modulation (LFM) waveform. This algorithm converts the extracted signal into a temporal classification problem and extracts the jamming-free segments of the signal to generate a band pass filter to suppress the ISRJ while retaining the real target signal components simultaneously.

### B. CRITICAL OVERVIEW OF AI APPLICATION

However, in order to predict the extent to which AI algorithm might be incorporated in the EW system, it is critical to assess the flip side of this technology. Some of the potentially destabilizing aspects of AI are discussed below:

1) AI based EW systems are susceptible to faulty date input, which can cause unexpected outcomes [50]. AI based techniques are heavily dependent on a large amount of data. Since data are collected from many sources, faulty data may result in flawed learning, thereby produces unintended consequences. Moreover, differentiating between similar objects may be challenging under denial and deception operations. Accidentally hitting the wrong targets could have strategic implications. So, the inherent problem of data reliability of AI raises a critical question about its loyalty on the battlefield. Some specific examples of this situation can be: AI technique that is used for classification of signals such as DNN requires a considerable amount of well labelled signal data for parameter optimization prior to implementation. However, the EW environment consists of very agile systems that can adapt and change. So, in this scenario, DNN performance will be uncertain if it is trained on less than the full range of possible data it might encounter. Similarly, in deep reinforcement learning algorithm, the parameter optimization data is built up over a very large number of interactions with the opponent system. However, EW does not allow repeated engagements with fixed rules for a long time. To an experienced EW operator, adversaries adapt rapidly by shifting tactics to different parts of the electromagnetic spectrum. Further, deep learning methods evolve with changing scenarios, and the possibilities of false targeting reduce.
2) One of the advantages of AI-enabled EW system is its speedy decision making. This can turn around into its disadvantage as well if it needlessly accelerates the growth of conflict from crisis to war. AI enable autonomous ISR systems could decrease the time available for diplomats to manage crises. Here, human intervention shall have a definite role to play.
3) Decisions of war and peace cannot be left to predictive analytic. Machine learning cannot reliably predict the exact outcomes of an event; rather, it can predict within margins of error. This margin of error may be tolerable for research purpose but not for the real-time battlefield. AI-enabled systems can correctly assess most but not all the situations. In military applications, this could mislead decision makers and put forces at risk.
4) AI-supported information warfare, including fake news, cybershots and deep fakes could deform public and leadership perceptions of international conflicts, thereby affecting strategic stability.

Despite the above limitations, researchers have focused on the strengths of AI and identified the opportunities and have enumerated sub-domains in EW where the application of AI shall have far-reaching consequences. Some examples include the application of AI techniques for improving DOA estimates for EW systems, classification of radar pulses, for adapting one's own communications to an EW environment where the opponent is using jamming, threat identification and analysis etc.

## IV. EW-AI SYSTEM

Appropriate application of AI in EW can help defence forces to spoil the attempts by the adversaries to hinder their communication networks including GPS, satellite signals etc. AI can reduce the cognitive burden and improve EW effectiveness for multi-domain operations. This will rank the incoming data quickly and accurately in order of priority to the warfighter so that less important signals can be removed. It is also useful in processing large volumes of data, thereby recognizing its patterns and deriving meaningful information. A generic block diagram of AI-enabled EW system is shown in Figure 11.

The antenna converts the received electromagnetic energy into an electrical signal so that it can be used by rest of the system. For ECM applications it converts electrical energy into specific slots of the electromagnetic spectrum to enhance warfighting potential. In figure 11, the search and tracking system is meant to continuously monitor the electromagnetic spectrum for locating hostile or friendly indications. It comprises of a receiver to identify the frequency of the transmitted signal, AOA of the signal in order to calculate the location of the transmitter. Analysis unit measures the values of signal parameters like PRF, pulse width, signal power, polarization, TOA and AOA etc. present in the received radar signal. This information is used to prepare a threat library

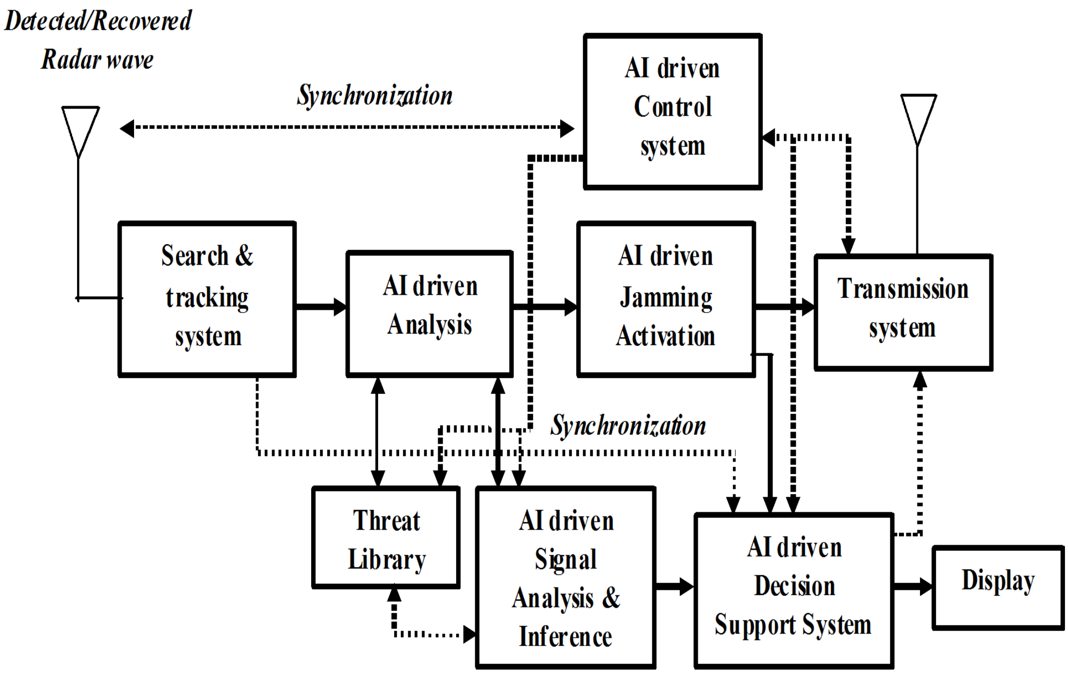

**FIGURE 11.** Basic block diagram of an AI based EW system.

in order to develop an EOB for situational awareness. Additionally, these are also used to develop new countermeasures. Signal analysis and inference unit may be AI driven. The function of signal analysis and inference module is to analyze the measured signal parameters in order to determine whether the received signal is from a hostile source or from a friendly source. This is accomplished by taking information about the hostile signal parameters from the threat library. Depending on the decision made by the analysis module, the jamming activation unit generates a suitable jamming signal. Thereafter, jammer antenna directs the jamming signal to the target. Control system can also be AI driven that works in synchronization with jammer transmission system, signal analysis and inference unit, threat library and radar signal receiving antenna. AI algorithm may be used in this module to allow entry of only hostile radar signal, thereby restricting the friendly communication signal. Thereafter, this hostile signal can be analyzed for extracting its parameter with the help of threat library and analysis module. A Suitable jamming signal can then be transmitted based on the decision of analysis modules to prevent threat radar from measuring target position and velocity. In general, if a ML/DL based AI system is used in EW block, its role is to provide a prediction of an evolving situation. It can be mathematically expressed using a generalized block diagram as shown in Figure 12. Let 'X' be an input signal applied to a ML/DL system (W). The output '$Y_0$' is expressed as

$$Y_0 = [X][W] \tag{23}$$

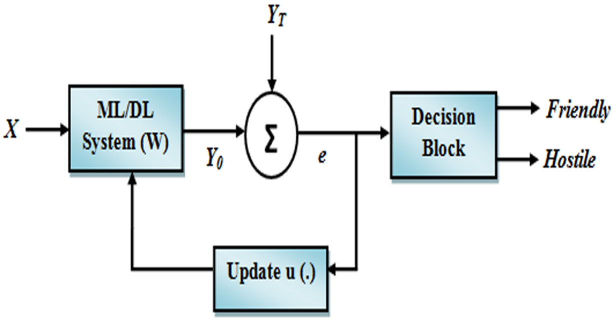

**FIGURE 12.** Generalized AI system.

For a supervised ML/DL system it is compared with an apriori target output $Y_T$. The error signal is expressed as

$$e = Y_0 - Y_T \tag{24}$$

The weight updation or adaptation of [W] is continued till the error is minimized. This is part of the supervised learning. For an unsupervised case $Y_0$ is fitted to a gaussian distribution and if it fulfills the standard deviation/variance requirements, the system is considered to have completed the training. After the training/learning phase is over, the output is passed through a threshold based decision block which categorizes the input signal as hostile or friendly.

A combination of advanced signal processing and intelligent AI-driven algorithms can help the military to detect variations in the threats caused by hostile adaptive radars and counter them. Additionally, these algorithms may enable

**TABLE 1. Performance accuracy of different AI techniques in EW.**

| AI Techniques Applications | EW categories | Accuracy/ related quality measures |
|---|---|---|
| CNN based PRI modulation type recognition [8] | ESM | 96.1% |
| CNN, SAE based radar signal recognition system [41] | ESM | 99.8% |
| Neural Network based radar signal emitter recognition and classification [26] | ESM | 84% |
| Hybrid classifier including CNN and ENN approach for radar waveform recognition [55] | ESM | 94.5% |
| GA-ANN based deception jamming detection system [46] | ECM | 95.2% |
| SVM based jamming style selection model [30] | ECM | 98.34% |
| DNN based system to determine the presence of jammer and its characteristics [40] | ECM | 85% |
| Machine learning algorithm including naive Bayesian classifier and ANN for threat detection, classification, and the selection of alternative countermeasures [7] | ECM/ESM | 96% |
| ANN based PRI modulation recognition [24] | ESM | 99% |
| DCNN and CDAE based radar signal intra-pulse modulation recognition [38] | ESM/ ECM | 95% |
| AI algorithm (ANN, SVM, DNN) for radar antenna scan parameter recognition [28] | ESM | 90% |
| PNN and WardŠs clustering based radar emitter signal identification and classification [25] | ESM | 100% |
| ANN, probability moment and ApEn for radar signal classification [27] | ESM | 99% |
| AI algorithm (NB, DT, ANN, and SVM)for radar antenna scan period estimation and radar antenna scan type recognition [29] | ESM | 97% |

EW systems to autonomously characterize these threats and generate effective countermeasures against them. It can also help in monitoring the effectiveness of one's own countermeasures so that other techniques can be adapted if they are either ineffective or if a hostile radar attempts to adapt around the responses. Intelligent AI-driven algorithm using ANN, DNN, a combination of ANN-GA or ANN-DNN technique can be used to analyze target radar signatures so as to identify and classify the emitters. These algorithms can also be used for detection of jammer and its characteristics and for developing efficient anti-jamming methods. Table 1 shows that AI technique that has been used for different applications in all the subdivisions of EW gives promising results.

Cognitive EW systems should be dynamic in nature with a closed loop feedback system. This will enable an intelligent response to defeat threat radars. Hence AI techniques can be a powerful tool for cognitive EW systems to exploit unknown radar signals. Moreover, a feedback mechanism could possibly co-ordinate the operations of the system's transmitter and receiver to achieve optimal jamming performance. With the help of machine learning and pattern recognition algorithms advance intelligent EW system may able to mimic human mental process of perception, memory, judgement and reasoning.

### A. EW - APPLICATION SPECIFIC AI TECHNIQUES

In this subsection, a few specific techniques related to active ECM, Passive ECM, and ECCM from state of the art in literature are discussed. Further, a few AI techniques that are suitable for specific EW applications are also enumerated.

- **ECM**: Most of the phenomena of ECM are time dependent, location dependent, and sometimes slow to fast varying, so for such diverse applications, a range of ML/DL tools may be considered. Here a few of the subdomains of ECM with respect to the application of ML/DL techniques are discussed. Jamming is a menace to radar system survival, and anti-jamming is one of the solutions. So, the classification of radar jamming is the first step toward anti-jamming. In this direction, a CNN based method for classification of radar jamming signal is discussed in [57]. In this method at first, a 1D-CNN is designed for radar jamming signal classification under the condition of sufficient training samples. Since the collection of sufficient training samples is time-consuming and expensive so to deal with this issue a CNN-based siamese network is then developed for radar jamming signal classification. Both of these methods have reported good classification accuracy. In [58] a new method of barrage jamming detection and classification for synthetic aperture radar (SAR) based on CNN is discussed. The method can effectively detect and classify the jamming in the low-frequency SAR signals. Two methods of predicting the appropriate jamming technique for a received threat signal using deep learning are presented in [59]. Firstly, a DNN is used on feature values extracted manually from the pulse description width (PDW) list of the radar signal. Secondly, long short-term memory (LSTM) is used that takes the PDW list as input. These deep learning models predict suitable jamming techniques for received threat signals without using the library. The prediction performance and time complexity of the two methods are then compared. It is reported that the prediction accuracy of the LSTM model is higher than the DNN model but the former requires longer training time. Chaff plays a significant role in EW [60]. Chaff clouds are an effective deception jamming technique for certain radars. It poses serious challenges to radar system performance. So, the study on radar characteristics of chaff clouds and countermeasures against chaff jamming is very crucial. In this direction, a technique of chaff jamming recognition based on the SVM classification method is presented in [60]. In [61], a method for recognizing radar compound jamming signals including additive, multiplicative and convolution signals of typical blanket jamming and deception jamming based on BP neural networks is discussed. At first, compound jamming signals are modelled with all received signals (echo, jamming and noise) in one PRI. Then features are extracted in time domain, frequency domain and fractal dimensions. Thereafter, classifier based on BP neural network is established to recognize types of compound jamming signals.

- **ECCM**: Frequency agile (FA) radar is useful for radar anti-jamming designs because of its ability to randomly alter the carrier frequency [62]. In this direction, a reinforcement learning-based anti-jamming frequency hopping algorithm for cognitive radar is presented in [62]. Q-learning and deep Q-network (DQN) is used in this method. It is reported that the learning performance of DQN is much better than that of Q-learning especially when the available frequencies are large. Radars resist interference by transmitting complex signals. Chaotic FM signal has high resolution in the time domain and Doppler frequency domain [63]. So, the chaotic FM signal is used to improve the ECCM capabilities of radar. However, the drawback is when the chaotic signal is applied to a pulse radar system; a randomly distributed range sidelobe appears. Hence, in a multi-target scenario, a high peak sidelobe of a strong target echo can mask the mainlobe of a weak target echo. This affects the dynamic range and increases the false alarm probability. In order to solve this issue, sidelobe suppression is necessary. In this direction, a sidelobe processing technique based on Radial Basis Function (RBF) network is discussed in [63]. The ability to discover targets at a great distance even in noisy environments is one of the key features of radar systems. So, for maintaining a high probability of detection and low false alarm rate CFAR detectors are used. Hence for lowering the false alarm rate, an ANN-based target detector with partial cell averaging constant false alarm rate (CA-CFAR) supervised training is presented in [64].

Among the ML/DL techniques the following are suitable:

1) ANN: It is a simplified mathematical analogue of human's neural network. It is used to process the input information by the layer-wise style for regression and classification tasks. ANN can learn by themselves and produce the output that is not limited to the input provided to them. Because of their parallel architecture, fault tolerance capacity, and ability to handle incomplete radar type descriptions and noisy data, ANN has been used for radar emitter recognition and identification process, jamming style selection etc [7], [24], [26], [29]. Moreover, ANN can be combined with other AI techniques like GA, DNN etc. to form a hybrid algorithm for developing jamming detection system, radar antenna scan parameter recognition etc [28], [46]. Performance of ANN based algorithms in various domains of EW in terms of accuracy is shown in Table 1.
2) CNN: DL based methods have achieved magnificent performance in speech, text and image processing [65]. CNN is a type of DL that have great advantages in extracting discriminant and static features of inputs. The robust feature extraction ability of CNN is inspired by neuroscience [35]. Moreover, CNN has been successfully applied in the field of radar jamming signal classification and in radar signal processing [8], [41], [57]. However, CNN-based methods usually need lots of training samples. So in a condition of limited training samples, Siamese-CNN (S-CNN) can be used [57]. Effectiveness of CNN based algorithms in terms of accuracy in various domains of EW in shown in Table 1
3) Long Short-Term Memory (LSTM): Traditional RNNs have a major setback called vanishing gradient, which leads to problems when processing long term dependencies in data [8]. To solve this issue, a modified architecture of RNN called LSTM was developed. LSTM is capable of learning long-term dependencies [35]. It is suitable to classify, process, and predict time series given time lags of unknown duration. LSTM is mainly used to solve the timing prediction problem because it can predict the state of the next moment based on the state of the data at the previous moment. Hence, it can be used for radar signal processing and for predicting the appropriate jamming technique [59].
4) Deep reinforcement learning (DRL): Reinforcement learning is an area of machine learning that is used

for taking suitable action to maximize the reward in a particular situation. It is employed to find the best possible behaviour or path that should be taken in a specific situation [39]. DRL is a combination of reinforcement learning and deep learning. Q- learning is the simplest reinforcement learning algorithm that seeks to learn a policy that maximizes the total reward [19]. A reinforcement learning algorithm that combines Q-Learning with deep neural networks is called as deep Q- network (DQN). DRL techniques can be used for developing anti-jamming algorithms for cognitive radar. Reinforcement learning based methods can help the radar in learning the jammer's strategies according to its own experience and then adopt a suitable strategy to avoid being jammed [62].

## V. CONCLUSION

Electronic Warfare is a critical enabling capability in military operations in both peace and war. Advances in digital technology have made it possible for modern military forces to develop highly resilient and adaptable electronic war-fighting systems with feedback that enable rapid adaptation to the electromagnetic environment. AI-based EW systems play a very significant role in this scenario. Because with AI, autonomous operations are facilitated, situational awareness increases and decision making becomes reliable. In this direction, an AI-enabled EW system can be effective in identifying the hostile radar emitters so as to determine the extent of lethality of the threat. Then depending upon the threat perception, a suitable AI-based counter strategy can be formulated to nullify the hostile EW threat. Furthermore, the information gathered during radar signal analysis can be used to prepare a threat library in order to develop an electronic order of battle (EOB) for situational awareness and develop flexible countermeasures as per the evolving EW scenario. In this way, an AI-based approach can provide battlefield planners with reliable tools for executing war-fighting efforts. The paper gives a brief review of EW's fundamental aspects and its components, the fundamental of some commonly used AI techniques, and the importance of AI techniques in modern EW systems. The work enumerates a list of EW and AI techniques that can be applied in an evolving scenario in the backdrop of changes taking place and the research that has been reported.

## REFERENCES

[1] N. Waghray, "Electronic warfare: The next step in national security," in *Proc. Annu. IEEE India Conf.*, Dec. 2011, pp. 1–5.

[2] L. Lazarov, "Perspectives and trends for the development of electronic warfare systems," in *Proc. Int. Conf. Creative Bus. Smart Sustain. Growth (CREBUS)*, Mar. 2019, pp. 1–3.

[3] S. D. Spiegeleire, M. Mass, and T. Sweijs, *Artificial Intelligence and the Future of Defense: Strategic Implications for Small-and Medium-Sized Force Providers*. Hague, The Netherland: HCSS, 2017.

[4] T. Singh and A. Gulhane. *8 Key Military Applications for Artificial Intelligence in 2018*. Accessed: Jan. 6, 2020. [Online]. Available: https://blog.marketresearch.com/8-key-military-applications-for-artificial-intelligence-in-2018

[5] M. Erenet, Y. B. Salman, and J. S. Park, "Clustering for electronic warfare information," in *Proc. 18th Int. Conf. Control, Autom. Syst. (ICCAS)*, 2018, pp. 1195–1197.

[6] S. Amuru, C. Tekin, M. van der Schaar, and R. M. Buehrer, "A systematic learning method for optimal jamming," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 2822–2827.

[7] S. Noh and U. Jeong, "Intelligent command and control agent in electronic warfare settings," *Int. J. Intell. Syst.*, vol. 25, no. 6, pp. 514–528, Jun. 2010.

[8] X. Li, Z. Huang, F. Wang, X. Wang, and T. Liu, "Toward convolutional neural networks on pulse repetition interval modulation recognition," *IEEE Commun. Lett.*, vol. 22, no. 11, pp. 2286–2289, Nov. 2018.

[9] A. M. Elbir, K. V. Mishra, and Y. C. Eldar, "Cognitive radar antenna selection via deep learning," 2018, *arXiv:1802.09736*. [Online]. Available: http://arxiv.org/abs/1802.09736

[10] H. Rahman, *Introduction to Electronic Defense Systems*. Boca Raton, FL, USA: CRC Press, 2019.

[11] M. S. K. Shankar and B. V. Mohan, "Recent advances in electronic warfare-esm systems," in *Proc. AECE-IRAJ Int. Conf.*, 2013, pp. 125–130.

[12] A. D. Martino, *Introduction to Modern EW Systems*. Norwood, MA, USA: Artech House, 2012.

[13] F. Neri, *Introduction to Electronic Defense Systems*, 2nd ed. Rijeka, Croatia: SciTech, 2006.

[14] M. Singh. *Electronic Warfare, Defence Scientific Information and Documentation Centre*. Accessed: 1988. [Online]. Available: Available:https://www.drdo.gov.in/sites/default/files/publcations-document/Electronic%20Warfare.pdf

[15] L. B. Van Brunt, *Applied ECM*, 1st ed. vol. 1. Dunn Loring, VA, USA: EW Engineering, 1978.

[16] F. A. Butt and M. Jalil, "An overview of electronic warfare in radar systems," in *Proc. Int. Conf. Technol. Adv. Electr., Electron. Comput. Eng. (TAEECE)*, 2013, pp. 213–217.

[17] P. M. Grant and J. H. Collins, "Introduction to electronic warfare," in *Proc. IEE F-Commun., Radar Signal Process.*, 1982, pp. 113–132.

[18] M. I. Skolnik, *Radar Handbook*, 3rd ed. New York, NY, USA: McGraw-Hill, 2008.

[19] S. Haykin, *Neural Networks: A Comprehensive Foundation*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 1999.

[20] Z. Boussaada, O. Curea, A. Remaci, H. Camblong, and N. M. Bellaaj, "A nonlinear autoregressive exogenous (NARX) neural network model for the prediction of the daily direct solar radiation," *Energies*, vol. 11, no. 3, pp. 620–641, Mar. 2018. [Online]. Available: http://dx.doi.org/10.3390/en11030620

[21] Y. E. Shao and S.-C. Lin, "Using a time delay neural network approach to diagnose the out-of-control signals for a multivariate normal process with variance shifts," *Mathematics*, vol. 7, no. 10, pp. 959–973, Oct. 2019. [Online]. Available: http://dx.doi.org/10.3390/math7100959

[22] K. Nikola, D. Medak, Z. Robert, and M. Rezo, "Machine learning methods for classification of the green infrastructure in city areas," *ISPRS Int. J. Geo-Inf.*, vol. 8, no. 10, pp. 1–14, 2019.

[23] S. Amuru and R. M. Buehrer, "Optimal jamming using delayed learning," in *Proc. IEEE Mil. Commun. Conf.*, Oct. 2014, pp. 1528–1533.

[24] Y. Liu and Q. Zhang, "An improved algorithm for PRI modulation recognition," in *Proc. IEEE Int. Conf. Signal Process., Commun. Comput. (ICSPCC)*, Oct. 2017, pp. 1–5.

[25] X. Liao, B. Li, and B. Yang, "A novel classification and identification scheme of emitter signals based on ward's clustering and probabilistic neural networks with correlation analysis," *Comput. Intell. Neurosci.*, vol. 2018, 2018, Art. no. 1458962, doi: 10.1155/2018/1458962.

[26] N. Petrov, I. Jordanov, and J. Roe, "Radar emitter signals recognition and classification with feedforward networks," *Procedia Comput. Sci.*, vol. 22, pp. 1192–1200, Jan. 2013.

[27] C. M. Jeong, Y. G. Jung, and S. J. Lee, "Neural network-based radar signal classification system using probability moment and ApEn," *Soft Comput.*, vol. 22, no. 13, pp. 4205–4219, Jul. 2018.

[28] T. Wan, X. Fu, K. Jiang, Y. Zhao, and B. Tang, "Radar antenna scan pattern intelligent recognition using visibility graph," *IEEE Access*, vol. 7, pp. 175628–175641, 2019, doi: 10.1109/ACCESS.2019.2957769.

[29] B. Barshan and B. Eravci, "Automatic radar antenna scan type recognition in electronic warfare," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 48, no. 4, pp. 2908–2931, Oct. 2012.

[30] X. Qiang, Z. Wei-gang, and B. Yuan, "Jamming style selection for small sample radar jamming rule base," in *Proc. IEEE Int. Conf. Signal Process., Commun. Comput. (ICSPCC)*, Sep. 2018, pp. 1–5.

[31] Y. Bengion and O. Delalleau, "On the expressive power of deep architectures," in *Proc. 14th Int. Conf. Discovery Sci.*, 2011, pp. 18–36.

[32] H. Yi, S. Shiyu, D. Xiusheng, and C. Zhigang, "A study on deep neural networks framework," in *Proc. IEEE Adv. Inf. Manage., Commun., Electron. Autom. Control Conf. (IMCEC)*, Oct. 2016, pp. 1519–1522.

[33] Y. Bengio, "Learning deep architectures for AI," *Found. Trends Mach. Learn.*, vol. 2, no. 1, pp. 1–127, 2009, doi: 10.1561/2200000006.

[34] Y. Bengio, P. Lamblin, and D. Popovici, "Greedy layer-wise training of deep networks," in *Proc. 20th Annu. Conf. Neural Inf. Process. Syst.*, 2007, pp. 153–160.

[35] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning: Adaptive Computation and Machine Learning Series*. Cambridge, MA, USA: MIT Press, 2016.

[36] G. Liu, H. Bao, and B. Han, "A stacked autoencoder-based deep neural network for achieving gearbox fault diagnosis," *Math. Problems Eng.*, vol. 2018, pp. 1–10, Jul. 2018, doi: 10.1155/2018/5105709.

[37] R. B. Palm, "Prediction as a candidate for learning deep hierarchical models of data," M.S. thesis, Tech. Univ. Denmark, Lyngby, Denmark, 2012.

[38] Z. Qu, W. Wang, C. Hou, and C. Hou, "Radar signal intra-pulse modulation recognition based on convolutional denoising autoencoder and deep convolutional neural network," *IEEE Access*, vol. 7, pp. 112339–112347, 2019, doi: 10.1109/ACCESS.2019.2935247.

[39] Y. Li, X. Wang, D. Liu, Q. Guo, X. Liu, J. Zhang, and Y. Xu, "On the performance of deep reinforcement learning-based anti-jamming method confronting intelligent jammer," *Appl. Sci.*, vol. 9, no. 7, pp. 3161–3176, 2019.

[40] S. Gecgel, C. Goztepe, and G. K. Kurt, "Jammer detection based on artificial neural networks: A measurement study," in *Proc. ACM Workshop Wireless Secur. Mach. Learn. (WiseML)*, 2019, pp. 43–48.

[41] J. Gao, Y. Lu, J. Qi, and L. Shen, "A radar signal recognition system based on non-negative matrix factorization network and improved artificial bee colony algorithm," *IEEE Access*, vol. 7, pp. 117612–117626, 2019, doi: 10.1109/ACCESS.2019.2936669.

[42] S. Salari, I.-M. Kim, F. Chan, and S. Rajan, "Blind compressive-sensing-based electronic warfare receiver," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 53, no. 4, pp. 2014–2030, Aug. 2017.

[43] S. You, M. Diao, and L. Gao, "Deep reinforcement learning for target searching in cognitive electronic warfare," *IEEE Access*, vol. 7, pp. 37432–37447, 2019, doi: 10.1109/ACCESS.2019.2905649.

[44] S. H. Chen, A. J. Jakeman, and J. P. Norton, "Artificial intelligence techniques: An introduction to their use for modelling environmental systems," *Math. Comput. Simul.*, vol. 78, nos. 2–3, pp. 379–400, Jul. 2008.

[45] N. Waghray and P. M. Menghal, "Simulation of radar topology networks to evolve the electronic warfare survivability metrics," in *Proc. 3rd Int. Conf. Electron. Comput. Technol.*, Apr. 2011, pp. 355–359.

[46] D. Wei, S. Zhang, S. Chen, H. Zhao, and L. Zhu, "Research on deception jamming of chaotic composite short-range detection system based on bispectral analysis and genetic algorithm–back propagation," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 5, pp. 1–11, 2019.

[47] J. R. Allen and G. Massolo, *The Global Race for Technological Superiority-Discover the Security Implications*. Milan, Italy: Ledizioni, 2019.

[48] J. E. Baker. *Artificial Intelligence and National Security Law: A Dangerous Nonchalance*. Accessed: Jan. 9, 2020. [Online]. Available: https://cis.mit.edu/publications/starr-forum-report/18-01-report

[49] Z. Shi, S. Tang, and X. Zhang, "Simulation of radar electronic warfare range of visualization applications," in *Proc. Int. Conf. Comput. Appl. Syst. Model. (ICCASM)*, Oct. 2010, pp. 93–96.

[50] Z. S. Davis, *Artificial Intelligence on the Battlefield—An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise*. Center for Global Security Research Lawrence Livermore National Laboratory. 2019. [Online]. Available: https://cgsr.llnl.gov/research/occasional-papers

[51] R. Brooks. *Technology and Future War Will Test US Civil-Military Relations*. Accessed: Jan. 9, 2020. [Online]. Available: https://warontherocks.com/2018/11/technology-and-future-war-will-test-u-s-civil-military-relations/

[52] Microwave and RF Staff. *BAE Bets on Use of Artificial Intelligence in Electronic Warfare*. Accessed: Jan. 9, 2020. [Online]. Available: https://www.mwrf.com/markets/defense/article/21849838/bae-bets-on-use-of-artificial-intelligence-in-electronic-warfare

[53] F. Wang, S. Huang, H. Wang, and C. Yang, "Automatic modulation classification exploiting hybrid machine learning network," *Math. Problems Eng.*, vol. 2018, pp. 1–14, Dec. 2018, doi: 10.1155/2018/6152010.

[54] J. Dudczyk and A. Kawalec, "Specific emitter identification based on graphical representation of the distribution of radar signal parameters," *Bull. Polish Acad. Sci. Tech. Sci.*, vol. 63, no. 2, pp. 391–396, Jun. 2015, doi: 10.1515/bpasts-2015-0044.

[55] M. Zhang, M. Diao, L. Gao, and L. Liu, "Neural networks for radar waveform recognition," *Symmetry*, vol. 9, no. 5, pp. 75–95, 2019.

[56] J. Chen, S. Xu, J. Zou, and Z. Chen, "Interrupted-sampling repeater jamming suppression based on stacked bidirectional gated recurrent unit network and infinite training," *IEEE Access*, vol. 7, pp. 107428–107437, 2019, doi: 10.1109/ACCESS.2019.2932793.

[57] G. Shao, Y. Chen, and Y. Wei, "Convolutional neural network-based radar jamming signal classification with sufficient and limited samples," *IEEE Access*, vol. 8, pp. 80588–80598, 2020, doi: 10.1109/ACCESS.2020.2990629.

[58] Y. Junfei, L. Jingwen, S. Bing, and J. Yuming, "Barrage jamming detection and classification based on convolutional neural network for synthetic aperture radar," in *Proc. IEEE Int. Geosci. Remote Sens. Symp. (IGARSS)*, Valencia, Spain, Jul. 2018, pp. 4583–4586, doi: 10.1109/IGARSS.2018.8519373.

[59] G.-H. Lee, J. Jo, and C. H. Park, "Jamming prediction for radar signals using machine learning methods," *Secur. Commun. Netw.*, vol. 2020, pp. 1–9, Jan. 2020, doi: 10.1155/2020/2151570.

[60] Y. Liu, S. Xing, Y. Li, D. Hou, and X. Wang, "Jamming recognition method based on the polarisation scattering characteristics of chaff clouds," *IET Radar, Sonar Navigat.*, vol. 11, no. 11, pp. 1689–1699, Nov. 2017.

[61] F. Ruo-Ran, "Compound jamming signal recognition based on neural networks," in *Proc. 6th Int. Conf. Instrum. Meas., Comput., Commun. Control (IMCCC)*, Harbin, China, Jul. 2016, pp. 737–740, doi: 10.1109/IMCCC.2016.163.

[62] L. Kang, J. Bo, L. Hongwei, and L. Siyuan, "Reinforcement learning based anti-jamming frequency hopping strategies design for cognitive radar," in *Proc. IEEE Int. Conf. Signal Process., Commun. Comput. (ICSPCC)*, Qingdao, China, Sep. 2018, pp. 1–5, doi: 10.1109/ICSPCC.2018.8567751.

[63] Q. Tan and Y. Song, "Sidelobe suppression algorithm for chaotic FM signal based on neural network," in *Proc. 9th Int. Conf. Signal Process.*, Beijing, China, Oct. 2008, pp. 2429–2433.

[64] J. Akhtar and K. E. Olsen, "A neural network target detector with partial CA-CFAR supervised training," in *Proc. Int. Conf. Radar (RADAR)*, Brisbane, QLD, Australia, Aug. 2018, pp. 1–6, doi: 10.1109/RADAR.2018.8557276.

[65] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015, doi: 10.1038/nature14539.

**PURABI SHARMA** received the B.E. degree in electronics and telecommunication engineering from GIMT, Guwahati, India, in 2011, and the M.Tech. degree in electronics and communication engineering from Gauhati University, Guwahati, in 2013. She is currently a Ph.D. Research Scholar with the Department of Electronics and Communication Engineering, Gauhati University. Her research interests include applications of soft-computational tools, bio-medical image processing, and signal processing.

**KANDARPA KUMAR SARMA** (Senior Member, IEEE) received the M.Tech. degree in digital signal processing from IIT Guwahati, India, in 2005, and the Ph.D. degree from the Department of Electronics and Electrical Engineering, IIT Guwahati. He is currently with the Department of Electronics and Communication Engineering, Gauhati University, India, as a Professor and the Head. He has authored ten books and several research articles. His research interests include applications of soft-computational tools, mobile communication, pattern recognition, and language technology. He is also a Fellow of IETE, India.

**NIKOS E. MASTORAKIS** (Senior Member, IEEE) received the B.Sc. (Ptychion) degree in pure mathematics, the B.Sc. and M.Sc. (Diploma) degrees in electrical engineering, and the Ph.D. degree in electrical engineering and computer science from the National University of Athens, Greece. He also studied medicine at the Medical School of Athens, National University of Athens. He had served as a Special Scientist on computers and electronics in the Hellenic (Greek) Army General Staff from 1993 to 1994 and taught several courses for the Department of Electrical and Computer Engineering, National Technical University of Athens, from 1994 to 1998. He was a Visiting Professor with the School of Engineering, University of Exeter, U.K., in 1998, and a Visiting Professor with the Technical University of Sofia, Bulgaria, from 2003 to 2004. He is currently a Professor with the Technical University of Sofia and the Department of Computer Science, Military Institutions, University Education (MIUE)–Hellenic Naval Academy, Greece. He was the first that solved with several different approaches to the former unsolved problem of multivariable factorization and published it. He was also the first scholar that completely solved the problem of stability for multidimensional systems using genetic algorithms. It was the first that constructed electronic musical instrument with the spaces of the Byzantine music. He is an Active Researcher in applied mathematics and computer science (systems theory, control, optimization theory, algorithms theory, signal processing, robotics, and computational intelligence). He has edited more than 200 books and authored five books. He has published more than 600 articles in international books, journals, and conferences. He is also a member of the New York Academy of Sciences, the A. F. Communications and Electronics Association, the American Association for the Advancement of Science, and other smaller scientific societies. He is also an active reviewer of 26 international journals, a member of the Editorial Board of 13 international journals, and an Editor of International Book Series: Editor of the series *Electrical and Computer Engineering* (WSEAS Press) and Editor of the series *Mathematics and Computers in Science and Engineering* (WSEAS Press). He is also a member of the Editorial Board of *Advances in Computation: Theory and Practice* (NOVA). He received several awards, including the Royal Society of England and the Hellenic National Research Foundation, for his academic studies and his scientific research. He is the Editor-in-Chief in many international journals. He was the General Chairman in more than 30 international conferences. He has organized more than 40 special sessions and three workshops and has given many plenary lectures. He is a registered Professional Electrical and Mechanical Engineer. He also received the Prize of Excellence from the Romanian Academy of Science, Bucharest, Romania.