Ekoloji 28(107): 153-164 (2019)

Support Vector Machine for Classification of Terrorist Attacks Based on Intelligent Tuned Harmony Search

Bing Bu [1], Zhenyang Pi [1], Lei Wang [2*]

[1] School of Economics and Management, Beihang University, Beijing 100083, CHINA

[2] Department of Public Order, Criminal Investigation Police University of China, Shenyang 110035, CHINA

[*] Corresponding author: leonwang521@126.com

Abstract

The classification of terrorist attacks plays an important role in ensuring optimal emergency resource allocation and effective implementation for contingency plan. This paper integrates support vector machine (SVM) with intelligent tuned harmony search (ITHS) to develop ITHS-SVM model for the classification of terrorist attacks, in which SVM provides learning and curve fitting functions while ITHS optimizes parameters of SVM. Through an experiment, the superiority of ITHS-SVM classification model on terrorist attack is verified with sample data of terrorist attacks in China during 2009-2016. Compared with six other classification models, ITHS-SVM exhibits the best performance on all four evaluation metrics of accuracy, precision, sensitivity and empirical error rate (EER). Our study demonstrates that ITHS-SVM model is effective for classification of terrorist attacks and can provide scientific basis for decision makers in response to terrorist attacks.

Keywords: terrorist attack, classification, support vector machine (SVM), intelligent tuned harmony search (ITHS)

Bu B, Pi Z, Wang L (2019) Support Vector Machine for Classification of Terrorist Attacks Based on Intelligent Tuned Harmony Search. Ekoloji 28(107): 153-164.

INTRODUCTION

Terrorist attacks cause great harm to people's lives, health and property and disrupt social order. In recent years, more and more terrorist attacks have taken place and various terrorist attacks continue to emerge, resulting in difficulties in prevention and control. Eight people were killed and almost a dozen injured when a 29-year-old man in a rented pickup truck drove down a busy bicycle path near the World Trade Center in Manhattan on November 1, 2017. More than 59 people have been killed and around 500 injured at an open-air country music festival in Las Vegas in the deadliest mass shooting in US history on October 2, 2017. At 21:20 on March 1, 2014, a group of individuals dressed in black clothes rushed into the square and ticket lobby of Kunming Railway Station to attack people indiscriminately. The assailants killed 31 people and injured 143 (including seven policemen). The July 2009 Urumchi riots were a series of violent riots over several days that broke out on July 5, 2009 in Urumchi, the capital city of Xinjiang Uyghur Autonomous Region (XUAR) in northwestern China.

How to quickly identify and classify terrorist attacks so as to take appropriate emergency measures is the foundation for implementing contingency plan and resource allocation. The management and disposal of terrorist attacks are very complicated which require proper planning and effective collaboration in order to minimize losses. Accurate classification on terrorist attack is the premise of formulating contingency plan, and is also the basis for rapid and scientific resource allocation by managers. Therefore, it is of great significance to study the classification problem of terrorist attacks, which ensures the rational implementation of contingency plan and rapid allocation of resources.

An emergency plan must be activated quickly at the very first time of a terrorist attack, which must be based on classifying the terrorist attack. Though the relevant information on the number of perpetrators, number of injured, number of fatalities, loss of property, and so on, is not very clear in the short period of time after the terrorist attack, but with current advanced surveillance and communication technology, an approximate estimate of such information can be obtained quickly. Thus the government can make a preliminary classification for the terrorist attack, and then activate the corresponding emergency plan. Of course, over

 Received: 7 Mar 2018 / Accepted: 28 Oct 2018

time, casualties, property losses and other information will dynamically update and tend to be accurate. If there is a significant change in some data, the terrorist attack classification must be updated in a timely manner, and the emergency response plan is adjusted accordingly.

The remainder of this paper is organized as follows. Relevant literature review on terrorist attacks and emergencies is given in Section 1.1, followed by the contribution of our study in Section 1.2. In Section 2, the proposed terrorist attack classification model is discussed and developed. Experimental results and performance evaluation by comparison analysis are given in Section 3, and conclusion is given in Section 4 with some suggestions.

Literature Review

Terrorism is calculated to create an atmosphere of fear and alarm through violence or threat of violence (Riley and Hoffman 1995). Terrorist attacks can cause mass casualties, infrastructure damage, or public concern with great impact. The motive of terrorist activist mainly comes from politics, religion, revenge, etc. The aim is not violence itself but to cause political and religious changes (Basuchoudhary and Shughart 2010, Kis-Katos et al. 2011).

The harmfulness of terrorist attack has aroused concern of many scholars, who have conducted research on technical means of response to terrorist attacks, psychology and behavior of terrorists, terrorism risk management (Milazzo et al. 2009, Woods 2011), resource allocation (Hupert et al. 2002), quick response simulation, situation evolution model based on stochastic Petri net, judgement on hub node of information dissemination, etc. (Kyle et al. 2004). In recent years, some scholars have studied terrorist attack and its related problems by using quantitative analysis approach. For example, Clauset et al. (2013) predicted the probability of large-scale terrorist attack in the future with statistical method based on historical data. The game theory was also adopted to identify the key members in a terrorist network. In addition, by using the center measure method of game theory, the intensity of interconnected subnetworks was assessed along with sensitivity analysis; thereby terrorists were classified (Linelauf et al. 2013, Husslage et al. 2015). In these studies, more quantitative analysis methods are used to study terrorist attacks, which provides the possibility of reducing the occurrence probability or the damage of terrorist attack. However, the literature on systematic classification (or grading) of terrorist attack is still relatively limited.

The United States pioneered the establishment of a five-level Homeland Security Advisory System, in which the degree of danger is marked from low to high with five colors of green, blue, yellow, orange and red, respectively (Guo 2004). The National Emergency Response Plan for Public Emergencies was issued in 2006 in China, where the public incidents are classified into four levels: level I (especially serious), level II (serious), level III (heavier) and level IV (average), indicated by red, orange, yellow and blue in turn.

The research on classification of emergencies in existing literature includes two levels: macro and micro levels. At the macro level, considering the hazard of incidents and government's control ability, classification models were established by using clustering and discriminant analysis, or support vector machine (SVM), and others. At the micro level, the emergencies were classified based on the level at which an incident occurs, the characteristics and type of industries in which an incident occurs, for example, the study on classification of major emergencies, or classification of road traffic emergencies. However, due to difficulty in data acquisition for different evaluation indices, classification decisions are made mainly based on intuition and experience of decision-makers, which cannot reflect the feature of incidents completely objectively.

Contribution

The terrorist attack is a kind of events with common characteristics. The problem of terrorist attack classification is provided to express the similarity of incidents so as to take action based on past experiences. Establishing an objective classification model of terrorist attacks based on characteristic data can provide scientific support for decision-making. Support Vector Machine (SVM) is an effective method for classification or grading problem (Vapnik 1998). SVM can perform fast iteration and calculation according to preset parameters. However the preset parameters may affect the accuracy of classification model, while Intelligent Tuned Harmony Search (ITHS) algorithm can overcome this shortcoming. Therefore, in this paper, we integrate SVM with ITHS to establish a classification model of terrorist attacks, called ITHS-SVM model. Sixty one terrorist attack samples are used to setup and test the proposed model with comparisons to other classification models. The results show that ITHS-SVM can classify and evaluate terrorist attacks effectively and quickly.

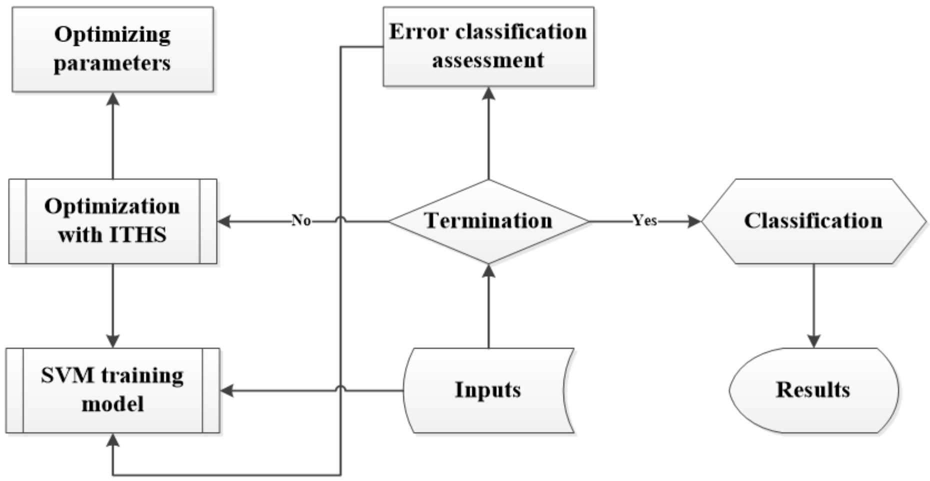

Fig. 1. Flowchart of ITHS-SVM classification model

ITHS-SVM CLASSIFICATION MODEL

ITHS-SVM classification model is able to determine the complex mapping relationship between input and output. The hyperplane is constructed in the feature space by support vector set comprising training data so as to form class labels, and then different class labels are used to classify data. Learning mechanism is also provided by the classification model, i.e., matching the hyperplane with training data through kernel function.

In the training process of SVM, the RBF (Radial Basis Function) kernel function can recognize support vector on function surface, and map sample data to high-dimension space non-linearly. Compared with other kernel functions, it can produce more reliable results. Therefore, it is more advantageous to select RBF as the kernel function of classification model (Hsu and Lin 2002). SVM requires selecting optimal parameters to ensure classification accuracy. The penalty parameter c and RBF's parameter γ should be optimized at the same time, so as to find the minimum number of support vectors and optimal parameters for classification.

The flowchart of ITHS-SVM classification model is shown in **Fig. 1**. The training sample is taken as inputs to train SVM model. In the training process, two key parameters of SVM, including the penalty parameter c and RBF's parameter γ, are optimized by ITHS. Whether the training process should be terminated or not is decided based on the error classification evaluation. Once the termination condition is satisfied, an optimal SVM classification model is fixed and the classification results are generated with slight deviation to the original classification.

Intelligent Tuned Harmony Search (ITHS)

Harmony search (HS) algorithm is an imitation of musician's improvisation for the best harmony (Geem et al. 2001). Each solution in HS algorithm is represented as a harmony by an n-dimension vector. The main steps of HS algorithm include initialization, harmony improvisation, harmony memory updating, and termination condition. In many different applications (Ceylan et al. 2016, Fattahi et al. 2015, Pahasa et al. 2014, Pereira et al. 2013), HS algorithm is combined with SVM to optimize the parameters of SVM so as to improve its performance. In this hybrid, the SVM parameter set is regarded as a harmony. An initial harmony population is generated at random. Then an iterative operation is carried out from the initial harmony population until the optimal parameter set for SVM model is found.

The effectiveness and efficiency of ITHS are better compared with HS algorithm. In ITHS, the harmony memory is divided into two sub harmony memories, A and B, where A comprises solution vectors whose objective function values are less than HM^{mean} (the mean fitness of all solution vectors in harmony memory), while B consists of other solution vectors. In ITHS, the value of PAR, a parameter representing the pitch adjustment rate of harmony vector, is updated dynamically with the number of iterations by the following iterative expression (Yadav et al. 2012):

$$PAR(Iter) = PAR_{max} - (PAR_{max} - PAR_{min}) \times \frac{Iter}{Iter_{max}} \quad (1)$$

where, $PAR(Iter)$ is the pitch adjustment rate at current iteration; PAR_{max} and PAR_{min} are the maximum and minimum pitch adjustment rates, respectively; $Iter$ is current iteration and $Iter_{max}$ is the maximum number of iterations. ITHS can solve high-dimension and local optimization problem effectively, and optimize parameters of SVM to overcome the shortcoming of SVM. Therefore, exploiting the advantages of SVM and ITHS, we construct the classification model of terrorist attack, in which SVM is used for learning, training and curve fitting, while ITHS is used for optimizing related parameters of SVM.

Classification Algorithm with SVM

In 1995, Cortes and Vapnik proposed SVM method in which input vectors are non-linearly mapped to a very high-dimension feature space. It is in fact a kind of machine learning method based on statistical theory. SVM is a supervised classification and regression method (Vapnik 1998), with the advantage of solving pattern recognition problem featured with small sample, nonlinearity and high-dimension space. It is to create a partitioned hyperplane to maximize the spacing between two classes for classification problem, which can be modeled as a quadratic programming. However, in practice, finding an appropriate hyperplane in the input space is restricted, so the input space is mapped to a high-dimension feature space so as to the optimal hyperplane can be found. Also, the hyperplane can be constructed by using kernel function method, where the optimal hyperplane is represented by the combination of input points, which is called Support Vector.

The principle of SVM is to construct a classification function based on input and output training data $(x_1, y_1), \dots, (x_n, y_n) \in R^m \times \{\pm 1\}$. The classification function distinguishes the training data by constructing a hyperplane equation, so that all points of the same class fall on the same side of the hyperplane. The classification situation is represented by maximizing the minimum distance between hyperplane and class. The minimum distance can be expressed by the geometric interval calculated by following formula:

$$y_i(w \cdot x_i + b) \geq -1, i = 1,2,\dots,m \tag{2}$$

where w is weight vector representing the function intervals from points with positive or negative value to 1. The optimal hyperplane, which maximizes the geometric interval between two parallel planes $w \cdot x + b = 1$ and $w \cdot x + b = -1$, is represented by $w \cdot x + b = 0$. The distance between two points in high-dimension space can be expressed by Euclidean distance. The Euclidean distance for maximum interval can be expressed by $2/\|w\|$, where $\|w\| = \sqrt{\sum_{i=1}^{m} w_i^2}$.

The classification problem in high-dimension space based on SVM can be represented by the following model:

$$\begin{aligned} &\min_{w,b} \frac{\|w\|^2}{2} \\ &s.t. y_i(w \cdot x_i + b) \geq 1 \end{aligned} \tag{3}$$

In some classification problems, the classes cannot be separated linearly. Instead, we need to construct an optimal plane for separation and add variable z_i to each point in the class to measure constraint variables. Thus, the classification problem is solved according to the following model:

$$\begin{aligned} &\min_{w,b} \frac{\|w\|^2}{2} + \frac{c}{m}\sum_{i=1}^{m} z_i \\ &s.t. \begin{cases} y_i(w \cdot x_i + b) + z_i \geq 1 \\ z_i \geq 0, i = 1,\dots,m \end{cases} \end{aligned} \tag{4}$$

where c is a penalty parameter selected by some optimization algorithm (ITHS is used in this paper). Model (4) can be solved by Lagrange multiplier method along with Kuhn-Tucker condition. Thus, the decision function can be represented by the following model:

$$\begin{aligned} f(x) &= sign(w \cdot x + b) \\ &= sign(\sum_{i=1}^{m} y_i \alpha_i k(x, x_i) + b) \end{aligned} \tag{5}$$

where, $k(x, x_i)$ is kernel function, and the parameters α_i and b are obtained from calculation of training data.

In our study, the kernel function is selected to construct the hyperplane for classification problem. A symmetric function that satisfies Mercer condition can be regarded as a kernel function. How to optimize the parameters of kernel function is the key to improve prediction accuracy. Commonly used kernel functions $k(x_i, x_j)$ include polynomial function, RBF and Sigmoid function, among which RBF can effectively map sample set from input space to high-dimension feature space to represent the complex nonlinear relationship between input and output. Therefore, study on the application of RBF as the kernel function in SVM model can effectively deal with the non-linear relationship between class tag and attribute (Huang et al. 2011, Pai et al. 2014). RBF kernel function is expressed as follows (Witten and Frank 2005):

$$k(x_i, x_j) = exp(-\gamma \|x_i - x_j\|^2) \tag{6}$$

where γ is a parameter embedded in RBF kernel function.

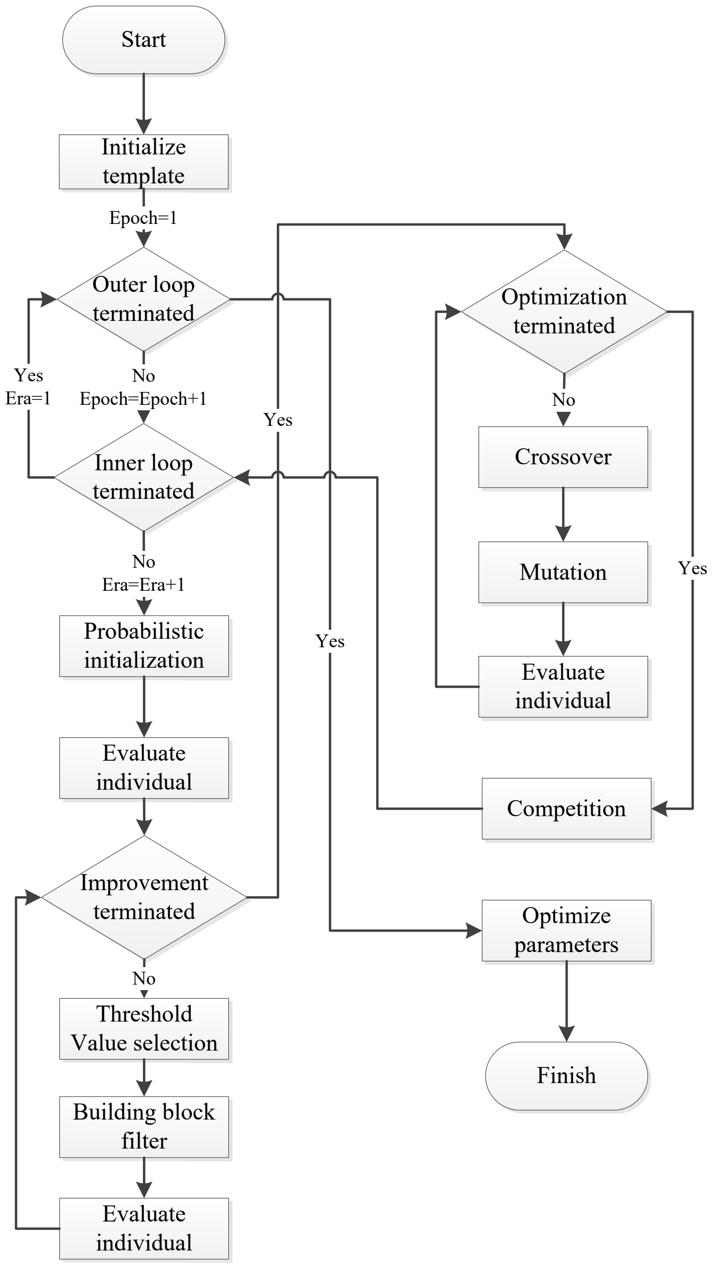

Fig. 2. Flowchart of ITHS-SVM classification model

SVM has unique advantages in solving small sample, nonlinear and high dimensional pattern recognition problems. SVM requires fewer samples because the key is to find the support vector, while the remote sample point outside the support vector is of little value. Because SVM is based on the principle of structural risk minimization, it has strong generalization ability and can overcome the problems faced by traditional algorithms such as the so-called dimensionality disaster and overfitting. In the existing literature, there is no general relationship between the minimum or optimal size of SVM training sample and the number of feature. In some applications involving SVM, the size of training sample can be as small as 30 (Liu et al. 2016) or even 20 (Cao et al. 2017).

Hybrid Algorithm of SVM with ITHS (ITHS-SVM)

The algorithm flow of ITHS-SVM is summarized in **Fig. 2**. This hybrid algorithm embeds two loops, the inner loop and the outer loop. The outer loop is used to obtain the optimal parameter setting for SVM, including the penalty parameter c and RBF's parameter γ. The inner loop constitutes the main body of ITHS, which consists of three phases, i.e., initialization phase, improvement phase and optimization phase.

Initialization phase

The initialization of ITHS-SVM algorithm is to generate an initial population, in which k building blocks are embedded. ITHS is used for carrying out a complete probabilistic initialization process, i.e., n harmony vectors with length of r_h are generated randomly. The size of initial population is determined by the following formula (Goldberg and Deb 1991):

$$n = \frac{\binom{l}{k}}{\binom{l-k}{\gamma_h - k}} 2c(\alpha)\beta^2(m-1)2^k \tag{7}$$

where l represents the length of vector, m represents the number of building blocks, and k represents the order of building block. $k < \gamma_h \leq l$. The value of γ_h can be chosen arbitrarily. Usually γ_h is set to $l - k$. $c(\alpha)$ denotes the normal random deviation with tail probability α, and β is the signal-noise ratio, i.e., the ratio of fitness value to difference between two competing building blocks. The setting of these parameters depends on specific problem.

After initializing the population with probability, individual in the population is evaluated, through which the fitness value of harmony vector is determined. The model accuracy can be improved by increasing the number of support vectors. The goal of ITHS-SVM model is to obtain acceptable prediction accuracy with minimum number of support vectors and optimal parameters in SVM.

Improvement phase

In improvement phase, the bad pitch in harmony string that doesn't belong to a building block is filtered out, so that the reserved population has a higher proportion of good pitch in building blocks. Threshold selection and building block filter are two commonly used methods in improvement phase. The threshold selection mechanism is used to limit competition between unshared building blocks. The threshold selection is more flexible than traditional championship selection which requires more pitches between two strings than expected. The threshold selection is represented by the following model:

$$\theta = \frac{\gamma_{h1}\gamma_{h2}}{l} \tag{8}$$

where θ is the threshold, and γ_{h1} and γ_{h2} are random strings with different lengths.

As for the building block filter, this method requires the string be constructed approximately with the length of problem in initialization phase. In order to enable ITHS better match function requirements, the initial length of string should be reduced to the length k of building block. The key to this process is to produce sufficient building block copies. One or more copies can be retained through random deletion, and be joined into subsequent process.

Optimization phase

The operators of ITHS mainly include crossover and mutation. Crossover operator is to optimize a harmony vector by changing different positions within it according to certain probability; while mutation operator is to prevent premature loss of individuals with important mark by generating random changes in different harmony vectors. In ITHS-SVM model, the parameters of SVM are adjusted by mutation operator, and the optimality of individual can be maintained by changing pitches in one or more harmony vectors with a certain probability.

Algorithm flow

The calculation process of support vector machine based on Intelligent Tuned Harmony Search is shown in **Fig. 2**.

EXPERIMENTAL RESULTS AND COMPARISON ANALYSIS

Sample Data

The experimental data comes from Global Terrorism Database (GTD) established by University of Maryland and United States Department of Homeland Security (DHS), which is an open database. In this paper parts of terrorist attack data in China are used to setup ITHS-SVM model on terrorist attack classification and test its performance. A total of 61 sample data of terrorist attacks from 2009 to 2016 in China is selected from GTD, among which 42 sample data during 2009-2014 are used as training sample and 19 sample data during 2015-2016 as test sample, as shown in **Table 1** and **Table 2**, respectively.

Since some indices of Chinese terrorist attack data are just in text format, it is necessary to collate text information into evaluable data. The selected terrorist attack data covers nine evaluation indices or attributes, including (1) attack type, (2) attack target, (3) weapon type, (4) number of perpetrators, (5) number of perpetrator fatalities, (6) number of civilian fatalities, (7) number of perpetrator injured, (8) number of civilian injured, and (9) property loss.

Table 1. Training sample: terrorist attacks during 2009-2014 in China

No.	Date	Location	Attack type	Attack target	Weapon type	Number of perpetrators	Number of perpetrator fatalities	Number of civilian fatalities	Number of perpetrator injured	Number of civilian injured	Property loss	Grade
1	20090316	Garzi, Tibet	7	8	5	8	0	0	0	0	1	3
2	20090319	Chongqing	9	9	6	2	0	1	0	0	2	3
3	20090401	Urumchi, Xinjiang	7	4	5	1	1	0	0	2	3	2
4	20090516	Mon Kok, HK	5	3	7	1	0	0	0	30	1	1
5	20090608	Mon Kok, HK	5	3	7	1	0	0	0	24	1	1
6	20090705	Urumchi, Xinjiang	9	3	4	3	0	184	0	0	4	4
7	20090909	Urumchi, Xinjiang	9	3	4	1	0	0	0	0	2	1
8	20100819	Akzo, Xinjiang	7	3	5	1	0	7	0	14	3	2
9	20110730	Kashgar, Xinjiang	7	3	5	2	0	0	0	0	2	1
10	20110730	Kashgar, Xinjiang	9	3	2	2	1	7	0	22	4	4
11	20110731	Kashgar, Xinjiang	9	4	4	2	5	6	0	10	4	4
12	20111027	Qamdo, Tibet	7	7	5	6	0	0	0	0	3	1
13	20120228	Yecheng, Xinjiang	9	4	4	3	7	15	0	14	3	4
14	20120510	Zhaotong, Yunnan	7	7	5	1	1	3	0	14	3	3
15	20120629	Khotan, Xinjiang	8	6	5	6	0	0	0	1	2	1
16	20121001	Yecheng, Xinjiang	5	8	2	1	1	0	0	0	1	1
17	20130309	Khotan, Xinjiang	6	8	3	2	0	0	0	0	2	1
18	20130626	Shanshan, Xinjing	9	8	3	5	2	4	1	4	3	4
19	20130626	Shanshan, Xinjing	9	8	4	5	2	4	1	4	3	4
20	20130626	Shanshan, Xinjing	9	7	3	5	2	4	1	4	3	4
21	20130626	Shanshan, Xinjing	9	4	3	5	2	4	1	4	3	4
22	20130626	Shanshan, Xinjing	9	4	3	5	2	4	1	4	3	4
23	20130626	Shanshan, Xinjing	9	4	3	5	2	4	1	4	3	4
24	20130628	Khotan, Xinjiang	9	8	4	100	0	0	0	0	4	3
25	20131028	Beijing	9	3	4	3	3	2	0	40	3	3
26	20131106	Beijing	7	3	5	1	0	1	0	8	2	4
27	20131117	Taiyuan, Shanxi	9	8	5	9	0	11	0	2	1	3
28	20131230	Kashgar, Xinjiang	9	8	5	8	8	0	0	0	2	3
29	20140113	Kaili, Guizhou	7	4	5	4	0	14	0	7	1	2
30	20140124	Aksu, Xinjiang	7	4	5	4	0	1	0	1	2	4
31	20140214	Wushi, Xinjiang	7	8	5	12	11	0	0	4	2	1
32	20140226	Hong Kong	9	7	4	2	0	0	0	1	1	4
33	20140301	Kunming, Yunnan	9	5	4	8	4	29	0	143	1	1
34	20140427	Kargilik, Xinjiang	8	8	4	4	0	3	0	0	1	4
35	20140430	Urumqi, Xinjiang	7	5	5	2	2	1	1	79	1	1
36	20140506	Guangzhou	8	5	4	4	0	0	0	7	1	4
37	20140513	Guma, Xinjiang	7	7	5	3	0	0	0	2	2	4
38	20140730	Kashgar, Xinjiang	4	7	4	3	0	1	0	0	1	4
39	20140820	Longkou, Shandong	9	5	3	1	0	1	0	19	2	3
40	20140921	Luntai, Xinjiang	7	8	5	40	10	3	0	14	2	1
41	20141012	Bachu, Xinjiang	9	7	5	4	4	18	0	24	1	1
42	20141128	Yarkant,Xinjiang	9	3	5	4	11	4	1	14	2	2

In the raw data, three indices of attack type, attack target and weapon type are specific textual description information. To facilitate evaluation and calculation, we assign certain values to these indices by using expert evaluation approach. More than 30 experts from public security colleges/universities/organs are selected to

Table 2. Test sample: terrorist attacks during 2015-2016 in China

No.	Date	Location	Attack type	Attack target	Weapon type	Number of perpetrators	Number of perpetrator fatalities	Number of civilian fatalities	Number of perpetrator injured	Number of civilian injured	Property loss	Grade	Test grade
1	20150213	Hotan, Xinjiang	7	8	5	1	1	7	0	7	1	1	1
2	20150306	Guangzhou	9	5	4	2	1	0	0	9	1	4	4
3	20150308	Yarkant, Xinjing	4	9	4	7	7	4	0	4	1	4	4
4	20150309	Hotan, Xinjing	3	8	4	4	0	0	0	0	1	4	4
5	20150312	Kashgar, Xinjing	9	4	5	6	4	0	2	10	2	4	4
6	20150422	Pishan, Xinjing	5	4	4	3	0	0	0	0	1	4	4
7	20150511	Hotan, Xinjing	7	8	5	1	1	2	0	0	1	4	4
8	20150512	Hotan, Xinjiang	7	8	5	2	2	1	0	4	1	4	4
9	20150526	Zawa, Xinjiang	7	8	5	6	2	0	0	0	1	3	**4**
10	20150617	Xian, Shaanxi	5	5	4	1	1	0	0	0	1	4	**2**
11	20150622	Kashgar, Xinjiang	9	8	5	15	15	18	0	5	1	1	**3**
12	20150720	Heze, shandong	7	3	5	1	1	2	0	23	1	2	2
13	20150729	Liuzhou, Guangxi	9	3	4	1	0	1	0	6	1	4	4
14	20150918	Terek, Xinjiang	9	4	5	4	0	50	0	0	1	2	**3**
15	20151206	Ejin Horo	5	8	4	5	0	0	0	13	2	4	4
16	20160428	Xian, Shaanxi	3	5	3	5	0	8	0	5	2	3	**4**
17	20161120	Wending, Yunnan	7	3	1	7	0	0	0	1	1	4	4
18	20161125	Hanzhong, Shaanxi	3	3	4	1	0	0	0	9	1	4	4
19	20161228	Karakax, Xinjiang	7	7	7	3	3	2	0	3	2	3	3

Source: Global Terrorism Database

establish evaluation criteria corresponding to different evaluation objects, and assign values to evaluation indices according to their importance or severity.

The attack type defined in the database includes armed assault, aircraft hijacking, explosion, infrastructure damage, unarmed assault, assassination, kidnapping, extortion and others, which are assigned values from 9 to 1 in turn according to the severity of incident.

The attack target includes army, public security organ, ordinary government sector, airport, transportation, commerce, private sector, non-governmental organization and others, which are assigned values from 9 to 1 in turn according to the importance of target under attack.

The weapon type includes nuclear weapon, biological weapon, chemical weapon, guns, explosive, melee, arson, vehicle and others, which are assigned values from 9 to 1 in turn according to the danger degree of weapon or tool used.

There is no standard encoding procedure that can be used for assigning numerical values to the three categorical indices of attack type, attack target and weapon target. Experts, based on experience, assign a larger value to an attack type, attack target or weapon type if it may cause more serious consequences. Therefore the numerical values assigned to attack type, attack target or weapon type do not have much significance in themselves, but by the relative magnitude of these values, the severity of the possible attack consequences can be indicated.

In the database, the property loss is described by four levels: particularly significant, significant, general and other, which are assigned values from 4 to 1 in turn.

According to National Emergency Response Plan for Public Emergencies of China, the public emergencies are divided into four levels of especially serious, serious, heavier and average, as grade 4, 3, 2, 1, respectively. Of course, this grading scheme is also used in classification of terrorist attacks.

Performance Evaluation Metrics

First, on the whole sample set with 61 terrorist attack cases, we adopt the 10-fold cross-validation (Kohavi, 1995) to test the performance of ITHS-SVM model. The whole sample set is randomly partitioned into 10 subsamples of approximately equal size. Of the 10 subsamples, a single subsample is retained as the validation data for testing the model, and the remaining 9 subsamples are used as training data. The cross-validation process is then repeated 10 times, with each of the 10 subsamples used exactly once as the validation data. The 10 results from the folds then are averaged to produce a single estimation on classification accuracy. The average accuracy is 89.2%. This shows that ITHS-SVM possesses high accuracy and generalization ability in the classification of terrorist attacks. Then, on the test sample containing 19 terrorist attack cases, the performance of ITHS-SVM is further evaluated.

Table 3. Confusion matrix

		Test grade	
		Positives	**Negatives**
Grade	Positives	a_1	b_2
	Negatives	b_1	a_2

The performance of classification model can be evaluated by computing the classified number correctly identified (denoted as true positives), unclassified number correctly identified (denoted as true negatives), incorrectly classified number (denoted as false positives) and incorrectly identified number (denoted as false negatives), which are represented by a_1, a_2, b_1, and b_2, respectively. The above four numbers constitute the so-called confusion matrix, as shown in **Table 3** (Sokolova and Lapalme 2009).

The confusion matrix is used to measure the accuracy, precision and sensitivity of classification model. The formulas for computing accuracy (A), precision (P) and sensitivity (S) are as follows:

$$A = \frac{a_1 + a_2}{a_1 + a_2 + b_1 + b_2} \quad (9)$$

$$P = \frac{a_1}{a_1 + b_1} \quad (10)$$

$$S = \frac{a_1}{a_1 + b_2} \quad (11)$$

Another comprehensive index for evaluating the performance of classification model is Empirical Error Rate (EER). EER for pairwise classification is defined as (Lee and Chen 2009):

$$EER_{ij} = \frac{e_{ij} + e_{ji}}{n_i + n_j}, 1 \le i < j \le C \quad (12)$$

where, n_i denotes the number of sample items of class i, and e_{ij} represents the number of sample items that originally belong to class i but are misallocated to class j; n_j denotes the number of sample items of class j, and e_{ji} represents the number of sample items that originally belong to class j but are misallocated to class i; C denotes the number of classes. EER_{ij} is used to measure the confusability between any two classes i and j. For class i, the higher the value of EER_{ij} is, the more confusable it will be with class j.

Experiment Results and Performance Evaluation

The key of ITHS-SVM model is to select a suitable classification function, which involves selection of kernel function and determination of penalty coefficient c. ITHS is adopted to adjust parameters c and γ so that ITHS-SVM model can attain the best performance. MATLAB is used for SVM programming with ITHS program embedded. The experimental environment is Pentium4/2.80 GHZ/2.24 GB/Windows 7 and Microsoft Visual C++ 2008.

Table 4. Comparisons with different classification models

Classsification model	Accuracy (%)	Precision (%)	Sensitivity (%)
ITHS-SVM	**91.22**	**93.16**	**95.33**
HSSVM	88.56	89.11	91.75
RS	87.22	88.00	91.73
SVM	87.11	87.54	91.71
ANN	87.50	89.40	89.60
C5.0	86.88	89.18	89.11
CART	82.55	83.12	88.94

The last column "test grade" in **Table 2** shows the classification results by ITHS-SVM on the test sample. Of the 19 test samples, 14 of the test grades are consistent with their original grades. The percentage of correct classification is 73.68%. Therefore, ITHS-SVM is effective for classification of terrorist attack.

To evaluate the performance of ITHS-SVM, we compare it with other six classification models, including HSSVM (Hyper-Sphere Support Vector Machines), RS (Rough Set), SVM, ANN (Artificial Neural Network), C5.0 decision tree (Schmueli et al. 2007) and CART (Classification and Regression Tree). There are some basic software systems available for these six classification models, which are developed based on Java, R, MATLAB or other languages. We adopt the basic algorithmic frameworks embedded in existing software packages to implement these six models and train them with the same training sample as ITHS-SVM. In our experiment, HSSVM and SVM adopt the RBF kernel function; RS produces classification decision rules based on attribute reduction; ANN adopts the most commonly used three-layer network with Sigmoid activation function and BP algorithm. C5.0 and CART belong to classification models based on Decision Tree algorithm. In our experiment, C5.0 adopts the "reduce-error" pruning technique while CART adopts the "minimum cost complexity" pruning technique when constructing decision trees. **Table 4** lists the accuracy, precision and sensitivity of various classification models on the same test sample. Among these models, ITHS-SVM possesses the highest accuracy, precision and sensitivity of 91.22%, 93.16 and 95.33%, respectively. This shows that ITHS-SVM has the best performance on terrorist attack classification compared with other models.

Further, the index EER is used to evaluate the performance of different classification models. **Fig. 3** depicts EERs with respect to different classification

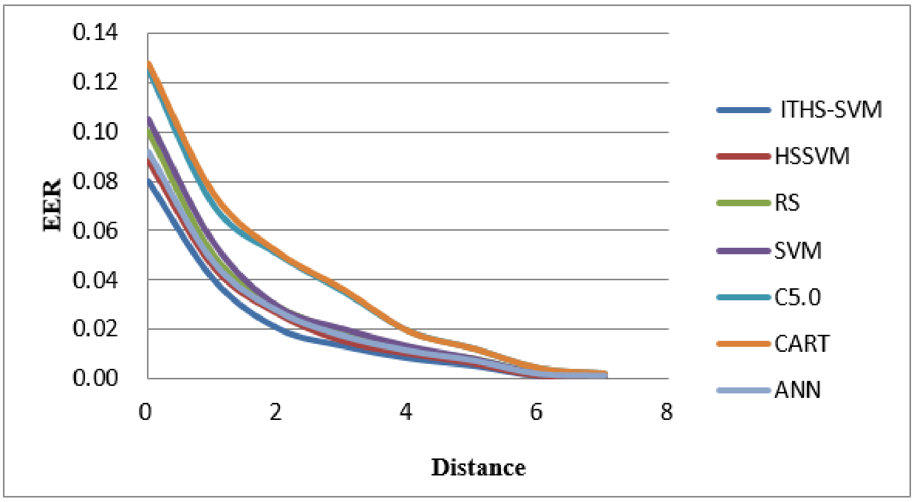

Fig. 3. EERs of various classification models

models, in which the horizontal coordinate represents Mahalanobis distance, while the vertical coordinate represents EER. **Fig. 3** shows that ITHS-SVM obtains the lowest EER. This demonstrates once again that ITHS-SVM possesses the best performance on terrorist attack classification compared with other models. From **Fig. 3**, we can also roughly characterize the relationship between two variables: class pair with shorter distance has higher EER; conversely, class pair with larger distance has lower EER.

From the above experiment results and comparison analysis, we can see that, as an objective quantitative method based on data support, though ITHS-SVM cannot be completely accurate for classification of terrorist attacks, but it has self-learning ability and flexible parameter adjustment ability, is easy to operate and improve, and can avoid arbitrariness of subjective judgment to some extent. Hence, it exhibits superior performance in classification of terrorist attacks.

CONCLUSION

In this paper, two methods of ITHS and SVM are combined to study the problem of terrorist attack classification. The principle and procedure of ITHS-SVM classification model are described. Through an experiment, the superiority of this classification model on terrorist attack is verified with sample data of terrorist attacks in China during 2009-2016. Compared with other classification models including HSSVM, RS, SVM, ANN, C5.0 and CART, ITHS-SVM shows the best performance on all four evaluation metrics of accuracy, precision, sensitivity and EER. When a terrorist attack happens, at the first time, it is necessary to quickly classify it on the basis of obtaining and roughly estimating relevant index data by means of on-site observation, video surveillance, etc., so as to initiate corresponding emergency response plan in time. As an effective objective classification method, ITHS-SVM can provide scientific basis for decision makers in response to terrorist attacks. Quick and correct classification is only one of the key efforts for emergency management of terrorist attacks. Some policy recommendations on the emergency management of terrorist attacks are given below.

First, the emergency management of terrorist attacks should be transformed from static and passive mode to dynamic and active mode. Therefore, it is necessary to promote the application of information technology in emergency management of terrorist attacks, so as to acquire real-time information and provide a basis for dynamic and active management.

Second, the emergency management of terrorist attacks should be transformed from extensive management to refined management. We should gradually realize the refined management based on socialization (for risk transfer), informatization (for foreknowledge, prejudgment and prevention), and legalization, and give full play to the role of informatization and intelligentization in emergency management of terrorist attacks.

Third, the emergency management of terrorist attacks necessitates acquisition and quantitative analysis of spatiotemporal information. We need to improve and implement effective spatiotemporal information collection, exploit measurable key element information to conduct prediction, prejudgment and early warning, realize whole process management covering information collection, information extraction, information classification, contingency plan, disposal and assessment, and utilize quantitative analysis technologies such as ITHS-SVM to drive closed-loop procedure management.

In the future, we will consider the background of big data era and further study terrorist attack classification according to historical statistics from the security sector of China.

REFERENCES

Basuchoudhary A, Shughart WF (2010) On ethnic conflict and the origins of transnational terrorism. Defence and Peace Economics, (21): 65-87.

Cao WD, Yan CP, Wu DJ, Tuo JB (2017) A novel multi-objective optimization approach of machining parameters with small sample problem in gear hobbing. International Journal of Advanced Manufacturing Technology, 93: 4099-4110.

Ceylan O, Taskin G (2016) SVM parameter selection based on harmony search with an application to hyperspectral image classification. In: IEEE (ed.), Proceedings of the 24th Signal Processing and Communication Application Conference (SIU), pp. 657-660, Zonguldak, Turkey, May 16-19.

Clauset A, Woodard R (2013) Estimating the historical and future probabilities of large terrorist events. The Annals of Applied Statistics, 7(4): 1838-1865.

Cortes C, Vapnik V (1995) Support-vector networks. Machine Learning, 20(3): 273-297.

Fattahi H, Gholami A, Amiribakhtiar MS, Moradi S (2015) Estimation of asphaltene precipitation from titration data: a hybrid support vector regression with harmony search. Neural Computing & Applications, 26(4): 789-798.

Geem ZW, Kim JH, Loganathan GV (2001) A new heuristic optimization algorithm: harmony search. Simulation, 76(2): 60-68.

Goldberg DE, Deb K (1991) A comparative analysis of selection schemes used in genetic algorithms. Foundations of Genetic Algorithms: 69-93.

Hsu CW, Lin CJ (2002) A simple decomposition method for support vector machines. Machine Learning, 46: 291-314.

Huang J, Bo Y, Wang H (2011) Electromechanical equipment state forecasting based on genetic algorithm-support vector regression. Expert Systems with Applications, 38: 8399-8402.

Hupert N, Mushlin A, Callahan MA (2002) Modeling the public health response to bioterrorism: using discrete event simulation to design antibiotic distribution centers. Medical Decision Making, (22): 1-9.

Husslage B, Borm P, Burg T (2015) Ranking terrorists in networks: A sensitivity analysis of Al Qaeda's 9/11 attack. Social Networks, 42: 1-7.

Jiao YB, Liu HB (2011) Application of genetic algorithm-support vector machine for damage identification of bridge. International Journal of Computational Intelligence and Applications, 10: 383-397.

Kis-Katos K, Liebert H, Schulze GG (2011) On the origin of domestic and international terrorism. European Journal of Political Economy, 27(1): 17-36.

Kohavi R (1995) The power of decision tables. Machine Learning: ECML-95: 174-189.

Kyle R, Via D, Lowy R (2009) A multidisciplinary approach to teach responses to weapons of mass destruction and terrorism using combined simulation modalities. Journal of Clinical Anesthesia, 16(2): 152-158.

Lee HS, Chen B (2009) Empirical error rate minimization based linear discriminant analysis. IEEE International Conference on Acoustics, 23(6): 1801-1804.

Lindelauf RHA, Hamers HJM, Husslage BGM (2013) Cooperative game theoretic centrality analysis of terorist networks: The cases of Jemash Islamiyah and Al Qaeda. European Journal of Operational Research, 229(1): 230-238.

Liu Z, Wang L, Zhang Y, Chen CLP (2016) A SVM controller for the stable walking of biped robots based on small sample sizes. Applied Soft Computing, 38: 738-753.

Milazzo MF, Ancione G, Lisi R (2009) Risk management of terrorist attacks in the transport of hazardous materials using dynamic geoevents. Journal of Loss Prevention in the Process Industries, 22(5): 625-633.

Pahasa J, Ngamroo I (2014) Adaptive power system stabilizer design using optimal support vector machines based on harmony search algorithm. Electric Power Components and Systems, 42(5): 439-452.

Pai PF, Huang KC, Lin KP (2014) Tourism demand forecasting using novel hybrid system. Expert Systems with Applications, 41: 3691-3702.

Pereira LAM, Papa JP, de Souza AN (2013) Harmony search applied for support vector machines training optimization. In: I. Kuzle, T. Capuder, H. Pandzic (eds.), Proceedings of IEEE EUROCON Conference, pp. 998-1002, Zagreb, Croatia, July 1-4.

Riley K, Hoffman B (1995) Domestic terrorism. A National Assessment of State and Local Preparedness, Santa Monica.

Shmueli G, Patel NR, Bruce PC (2007) Data mining for business intelligence. John Wiley and Sons, New Jersey.

Sokolova M, Lapalme G (2009) A systematic analysis of performance measures for classification tasks. Information Processing and Management, 45: 427-437.

Vapnik VN (1998) Statistical Learning Theory. John Wiley, New York.

Witten IH, Frank E (2005) Data mining: practical machine learning tools and techniques with Java Implementations. Morgan Kaufmann, San Francisco.

Woods J (2001) The 9/11 effect: Towards a social science of the terrorist threat. The Social Science Journal, 48: 213-233.

Yadav P, Kumar R, Panda SK (2012) An intelligent tuned harmony search algorithm for optimization. Information Sciences, 196: 47-61.