ECTI Transactions on Computer and Information Technology
Journal homepage: https://ph01.tci-thaijo.org/index.php/ecticit/
Published by the ECTI Association, Thailand, ISSN: 2286-9131

Stacking Ensemble Learning with Regression Models for Predicting Damage from Terrorist Attacks

Thitipong Kawichai[1]

ABSTRACT

Terrorist attacks can cause unexpectedly enormous damage to lives and property. To prevent and mitigate damage from terrorist activities, governments and related organizations must have suitable measures and efficient tools to cope with terrorist attacks. This work proposed a new method based on stacking ensemble learning and regression for predicting damage from terrorist attacks. First, two-layer stacking classifiers were developed and used to indicate if a terrorist attack can cause deaths, injuries, and property damage. For fatal and injury attacks, regression models were utilized to forecast the number of deaths and injuries, respectively. Consequently, the proposed method can efficiently classify casualty terrorist attacks with an average area under precision-recall curves (AUPR) of 0.958. Furthermore, the stacking model can predict property damage attacks with an average AUPR of 0.910. In comparison with existing methods, the proposed method precisely estimates the number of fatalities and injuries with the lowest mean absolute errors of 1.22 and 2.32 for fatal and injury attacks, respectively. According to the superior performance shown, the stacking ensemble models with regression can be utilized as an efficient tool to support emergency prevention and management of terrorist attacks.

Article information:

Keywords: Damage, Ensemble Learning, Stacking Model, Terrorist Attack, Terrorism

Article history:
Received: December 31, 2023
Revised: April 12, 2024
Accepted: May 8, 2024
Published: May 18, 2024 (Online)

DOI: 10.37936/ecti-cit.2024183.255276

1. INTRODUCTION

Terrorism is one of the most desperate threats to the security of nations [1]. Terrorist attacks can endanger unexpectedly massive damage to lives and properties. To prevent and mitigate damage from terrorism, governments and related organizations must have effective measures and efficient tools for tackling terrorist attacks.

With the advent of open terrorism data in the global terrorism database (GTD) [2], machine learning (ML) has been introduced for systematically analyzing and forecasting terrorism in many works. To support decision-making in preventing and countering terrorism, existing ML-based methods were proposed for predicting different attributes of future terrorist attacks, such as locations susceptible to terrorism [3-5], attack types [4, 5], targets [6], weapons [4, 5], terrorist groups behind a particular attack [7], the suicide of terrorists [4], and the success of attacks [4, 5, 7].

For controlling and responding to emergencies of terrorist incidents, rapid and accurate estimates of consequences from terrorist attacks are necessary [8]. Due to the potentiality of ML, the ML approach has been applied to forecast consequences (e.g., the number of fatalities and injuries) of various emergencies, such as earthquakes [9, 10], steel plant accidents [11], and coal mine gas accidents [12], to support decision-making in emergency management. Meanwhile, there are only a few ML models for predicting the outcomes of terrorist attacks. For example, Feng *et al.* proposed a binary classification model based on the extreme gradient boosting (XGBoost) model to predict whether a terrorist attack will cause casualties or not [13]. To enhance the previous casualty prediction of terrorist attacks, Hu *et al.* created the two-step ML method, which utilized the multilayer perceptron and random forest model for estimating the number of civilian fatalities and injuries resulting from terrorist attacks [14].

To improve the consequence prediction of terrorist attacks, a stacking ensemble method with regression

[1] The author is with the Department of Mathematics and Computer Science, Academic Division, Chulachomklao Royal Military Academy, Nakhon Nayok, Thailand 26001. E-mail: thitipong.kaw@crma.ac.th
[1]Corresponding author: thitipong.kaw@crma.ac.th

was proposed in this work for predicting damage from terrorist attacks. In addition to estimating the number of causalities caused by a particular attack, the proposed method can predict if that terrorist attack can cause property damage. The proposed method combines classification and regression techniques in ML to enhance the accuracy of damage prediction resulting from terrorist attacks. First, three stacking ensemble models were developed to preliminarily classify terrorist attacks that can cause fatalities, injuries, or property damage. For fatal and injury attacks, two independent regression models were used to predict the number of deaths and injuries caused by terrorist attacks, respectively.

2. RELATED WORKS

The availability of open terrorism data provides more opportunities to study and research on terrorist attacks. To learn these complex data of terrorist incidents, many computational methods based on data mining and machine learning (ML) have been recently proposed for different purposes, including analysis of terrorism data and prediction of terrorist attacks.

To better comprehend terrorist attacks, Guohui *et al.* utilized correspondence analysis to uncover the relationships between the characteristics of terrorist attacks and the levels of fatalities. They found that locations, weapons, targets, and attack types were the significant factors influencing fatalities [15]. Li *et al.* quantitatively studied the temporal and spatial evolution of terrorism by applying the k-means algorithm for clustering terrorist attacks and analyzing the top five clusters selected according to the damage levels [16]. From the analysis, it was found that the regions that will seriously face terrorist attacks in the future are Southeast and Central Asia, the Middle East, and Africa. Understanding past terrorist incidents would help set policies to prevent and counter future terrorist activities.

Due to the prediction power of ML, various ML models have been applied for predicting numerous attributes of terrorist attacks. Agarwal *et al.* utilized support vector machine (SVM), random forest (RF), naïve Bayes (NB), and logistic regression (LR) for predicting the success of terrorist activities and terrorist groups behind terrorist attacks [7]. Uddin *et al.* created deep neural network models for predicting five attributes of terrorist attacks, including the success of terrorist attacks, the suicide of terrorists, attacked regions, weapons, and attack types [4]. Olabanjo *et al.* proposed an ensemble ML model based on SVM and k-nearest neighbors (KNN) to identify risk regions of terrorism [3]. Saidi and Trabelsi developed a deep learning model that combines convolutional neural network (CNN) and long short-term memory (LSTM) for predicting multiple characteristics of future terrorist attacks, such as attack success, attacked regions, attack types, and weapon types [5].

To support decision-making for preventing and managing emergency consequences of terrorist events, predictive models for estimating damage from terrorist attacks are required. Jun *et al.* proposed a classification model for hazard grading of terrorist attacks using principal component analysis (PCA), k-means clustering, and the entropy method [17]. Feng *et al.* introduced a casualty classification model, named RP-GA-XGBoost, to predict whether terrorist attacks will cause fatalities or injuries to innocent people or not [13]. In this model, RF and PCA were utilized for feature selection, and the genetic algorithm (GA) was applied to choose parameter values of the extreme gradient boosting model (XGBoost). Consequently, RP-GA-XGBoost achieved an accuracy of 86% in classifying casualty terrorist attacks, but it cannot estimate the number of casualties. To enhance the casualty prediction, Hu *et al.* proposed the two-step method, which incorporates a back propagation neural network and RF, to predict the number of deaths and injuries resulting from terrorist attacks [14]. The results showed that the two-step model can efficiently forecast the number of fatalities and injuries with low mean absolute errors (MAE) of 1.67 and 4.13, respectively. However, only a few methods currently exist for predicting damage from terrorist attacks, and there is still room to improve the predictive capacity of the models.

3. MATERIALS AND METHODS

3.1 Data Collection and Filtering

The terrorism data were downloaded from the Global Terrorism Database (GTD) at `https://www.start.umd.edu/gtd`, a database containing information on more than 200,000 violent and terrorist incidents that occurred around the world [2]. To filter only the acts of terrorism, the incidents tagged with doubt of terrorism inclusion were excluded from the study. Additionally, the incidents with unknown numbers of deaths and injuries were removed. Consequently, 81,526 records of terrorist attacks remained for data pre-processing.

3.2 Data Pre-Processing

In this step, the downloaded data were prepared in a suitable format for input to ML models. The processes of data pre-processing include dealing with redundant features and missing values, data encoding, and data normalization.

1) Dealing with Redundant Features and Missing Values

In the downloaded data set, there are some redundant features, such as country IDs, country names, attack type IDs, and names of attack types. In the case of redundant features, only features with texts were kept, such as country names and names of attack types. In the case of missing data, the most frequent value of a feature (mode) was used to fill in missing values.

2) Data Encoding

This process is for converting categorical features to numerical values. In the terrorism data, the categorical features are country names, attack types, target types, terrorists/groups, and weapon subtypes. Each categorical feature was transformed by one-hot encoding, as illustrated in Figure 1.

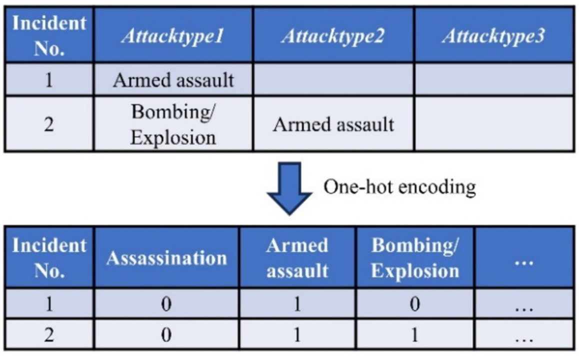

Fig.1: *An example of data encoding.*

For each incident, information about used attack types was transformed into a binary vector containing values of ones at the places of attack types used and values of zeros at the others. For example, in incident no. 1, only the attack type "Armed assault" was employed. Thus, the binary vector representing the attack type information of incident no. 1 contains one at the position of "Armed assault". For incident no. 2, there were two attack types recorded including "Bombing/Explosion" and "Armed assault". Therefore, the binary vector collecting the attack type information of incident no. 2 contains the values of ones at the positions of "Bombing/Explosion" and "Armed assault".

For each terrorist attack, at most three attack types, three target types, and four weapon subtypes were recorded. By the one-hot encoding used in this work, all recorded attack types, target types, and weapon subtypes can be retained and encoded. This differs from existing methods which can keep only a single attack type, target type, and weapon type or subtype.

3) Data Normalization

After data encoding, the values of most features except incident dates, latitudes, and longitudes were in a range of 0 to 1. Thus, the incident dates, latitudes, and longitude values were normalized to ensure that all features were on a similar scale. In the case of incident dates, the data of day ($iday$), month ($imonth$), and year ($iyear$) of an incident were initially converted to a floating number of the time point (timepoint) as written in (1), where $ndays$ is the number of days in the year until the day of the incident, and $ndays_{total}$ is the total number of days in the year. Then, time points, latitudes, and longitudes of all terrorism incidents were normalized using min-max normalization, as described in (2), where x and x_{new} are an original value and a normalized value, respectively. Regarding a certain feature, min and max represent the minimum value and maximum value of that feature, respectively.

$$timepoint = iyear + \frac{ndays}{ndays_{total}} \tag{1}$$

$$x_{new} = \frac{x - \min}{\max - \min} \tag{2}$$

4) Data Matrix Creation

The summary of data features after data encoding and normalization is shown in Table 1. In total, there are 21 features, and all of them are numeric. The size of a feature refers to the size of a vector or the number of elements that a vector contains for retaining the feature information of an incident. For example, a vector with a length of 164 can represent the country where an incident occurred. Thus, an $n \times 164$ data matrix retains the countries where n terrorism incidents occurred.

In Table 1, the first 16 features were used as independent variables. To create a data matrix of independent variables (X), the data matrix of each feature was concatenated together. Consequently, X which is an $n \times 821$ matrix containing numeric values in a range of 0 and 1 was obtained to retain features' values of n terrorism incidents.

In classifying terrorist attacks, $isKilled$, $isInjured$, and $isPropDamage$ were target variables. To construct three independent binary classifiers, data of each target variable were stored in a binary vector with the size of n, denoted as y_c. In regression analysis, two numerical features ($nKilled$ and $nInjured$) were defined as target variables. Data of each target variable were saved in y_r, a numeric vector with the size of n, and used to build a regression model to predict the number of fatalities or injuries. It should be noted that the number of deaths and injuries in this work were from only killed and injured innocent people and did not include deaths and injuries of terrorists.

3.3 Development of Stacking Ensemble Classifiers with Regression Models

An overview of the stacking ensemble learning method with regression models for predicting damage from terrorist attacks is illustrated in Figure 2. In the proposed method, classification and regression techniques were utilized together to enhance prediction accuracy.

In the classification stage, three stacking ensemble models, including a fatal attack classifier, an injury attack classifier, and a property damage attack classifier, were independently created and used to classify terrorist attacks. Each stacking ensemble classifier is

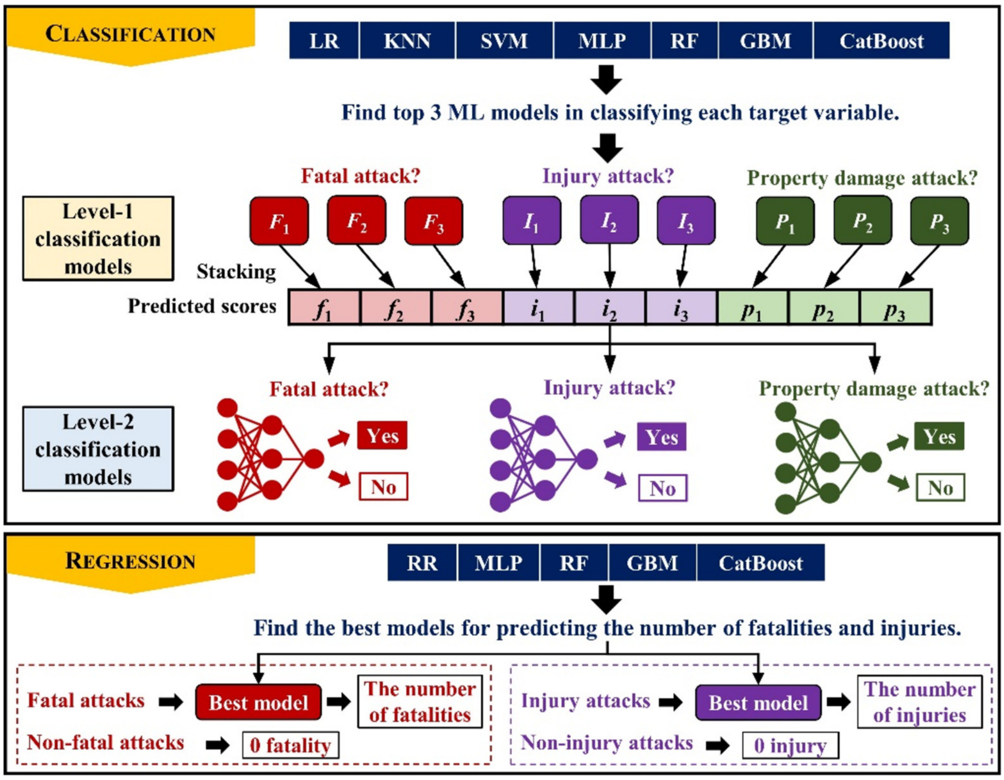

Fig.2: *An overview of the proposed method.*

Table 1: *Summary of data features.*

No.	Feature Name	Size	Description
1	*multiple*	1	Was the attack part of a multiple incident?
2	*norm_timepoint*	1	The normalized time point when the incident occurred
3	*extended*	1	Was the incident extended more than 24 hours?
4	*country*	164	The country where the incident occurred
5	*norm_latitude*	1	The normalized latitude
6	*norm_longitude*	1	The normalized longitude
7	*vicinity*	1	Did the incident occur in the vicinity of the city?
8	*attack_types*	9	Attack types used
9	*target_types*	22	Target types
10	*weapon_subtypes*	39	Weapon subtypes used
11	*terrorists*	576	Persons or groups that carried out the attack
12	*individual*	1	Did an individual carry out the attack?
13	*success*	1	Did the attack succeed?
14	*suicide*	1	Was there a terrorist suicide?
15	*claimed*	1	Was there a group that claimed responsibility for the attack?
16	*ishostkid*	1	Was there a hostage kidnapping?
17$^{(C)}$	*isKilled*	1	Was there a fatality?
18$^{(C)}$	*isInjured*	1	Was there an injury?
19$^{(C)}$	*isPropDamage*	1	Was there property damage?
20$^{(R)}$	*nKilled*	1	The number of fatalities
21$^{(R)}$	*nInjured*	1	The number of injuries

$^{(C)}$ is marked for a target variable in the classification.
$^{(R)}$ is marked for a target variable in the regression.

defined as a two-layer classification model. To appropriately choose ML models for developing the level-1 classifiers, seven ML algorithms, including logistic regression (LR) [18], k-nearest neighbors (KNN) [19], support vector machine (SVM) [20], multilayer perceptron (MLP) [21], random forest (RF) [22], gradient boosting machine (GBM) [23], and categorical boosting (CatBoost) [24], with default values of all hyperparameters were tested and evaluated their performance in the classification of fatal, injury, and property damage attacks.

Since a stacking model discards the features of original data and mainly relies on the classification results of base models, the poor predictions from base models can negatively influence the performance of the stacking model [25]. The top three best ML algorithms were used in the level-1 classification models to create a stacking model for each classification type. In Figure 2, F_j, I_j, and $P_j (j = 1, 2, 3)$ represent the top three best ML models in classifying fatal, injury, and property damage attacks, respectively. For each terrorist attack, nine classifiers in the level-1 classification generate nine predicted scores, which are the predicted scores obtained from the level-1 fatal attack classifiers (f_j), injury attack classifiers (i_j), and property damage classifiers (p_j), where $j = 1, 2, 3$. These predicted scores were concatenated together to create a vector with the size of nine and served as an input for the level-2 classification models.

In the level-2 classification, three MLP models were independently built for classifying fatal attacks, injury attacks, and property damage attacks based on the stacking features of nine predicted scores from the level-1 classifiers. Due to the small size of inputs, MLP with a single hidden layer was utilized. In tuning parameter values of each MLP model, the number of hidden nodes was varied as 3, 5, 7, 9, 11, and 13. The prediction results obtained from the level-2 classification are three binary target variables indicating an attack is fatal or non-fatal, injury or non-injury, and property damage or non-property damage. For non-fatal and non-injury attacks, the predicted values of fatalities and injuries were set as 0. For fatal or injury attacks, regression models were built and used to estimate the number of deaths or injuries. In the selection of ML models for the regression analysis, five regression algorithms, including ridge regression (RR) [26], MLP [21], RF [22], GBM [23], and CatBoost [24], were tested and compared their performance in predicting the number of fatalities and injuries from terrorist attacks. The best model for each regression case was selected and used in the proposed method.

3.4 Performance Evaluation

The performance of the proposed method was evaluated in both classification and regression steps by performing 10-fold cross-validation, as illustrated in Figure 3.

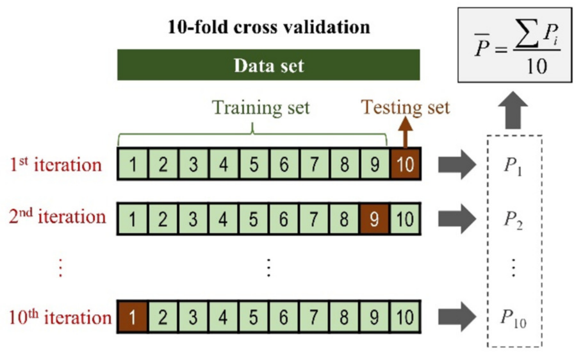

Fig.3: *Illustration of 10-fold cross-validation.*

Initially, a data set was approximately equally divided into ten subsets. In each iteration, nine of them were used to train a model. Then, the remaining subset of data was used to test the model and calculate the value of performance measure (P_i), where $i = 1, 2, \dots, 10$. The average value of a performance measure ($\bar{P}$) represents the estimated performance of a model. In tuning the parameter values of models, 10% of the data in a training set were randomly selected and served as a validation set. The remaining data in that training set were used to train a model.

In the classification of terrorist attacks, the standard performance measures including precision (PRE), recall (REC), accuracy (ACC), F1-score (F1), and Matthew's correlation coefficients (MCC) were calculated as shown in (3) – (6), where TP, FP, TN, and FN represent the number of true positives, false positives, true negatives, and false negatives, respectively. Furthermore, the area under a receiver operating characteristic curve (AUC) and the area under a precision-recall curve (AUPR) were computed to evaluate the overall performance of classification models.

$$\text{PRE} = \frac{TP}{TP+FP}, \quad \text{REC} = \frac{TP}{TP+FN} \tag{3}$$

$$\text{ACC} = \frac{TP+TN}{TP+TN+FP+FN} \tag{4}$$

$$\text{F1} = \frac{2 \times \text{PRE} \times \text{REC}}{\text{PRE}+\text{REC}} \tag{5}$$

$$\text{MCC} = \frac{TP \times TN - FP \times FN}{\sqrt{(TP+FP)(FN+TN)(TP+FN)(FP+TN)}} \tag{6}$$

In the regression step, the performance of a regression model was evaluated by using mean absolute errors (MAE) as shown in (7), where y_i is the actual number of fatalities or injuries, $\hat{y}_i$ is the predicted number of fatalities or injuries, and n is the number of testing samples.

$$\text{MAE} = \sum_{i=1}^{n} \frac{|y_i - \hat{y}_i|}{n} \tag{7}$$

4. RESULTS AND DISCUSSION

4.1 Preliminary Data Analysis

In the pre-processed data set, there were 81,526 terrorist attacks retained for use in this work. The percentages of terrorist attacks which caused fatalities, injuries, and property damage are summarized in Figure 4. The number of fatal, injury, and property damage attacks are 35,702 (43.8%), 30,631 (37.6%), and 35,695 incidents (43.8%), respectively. Additionally, 9,576 incidents, up to approximately 12%, were serious terrorist attacks that caused damage to both lives and property.

Furthermore, the number of fatalities and injuries caused by terrorist attacks were summarized using basic descriptive statistics in Table 2. Consequently, a terrorist attack causes 1.46 deaths and 2.80 injuries of civilians on average with standard deviations (SD) of 9.15 and 57.06, respectively. More than 50% of terrorist attacks are non-fatal and non-injury attacks (Figure 4). Thus, the minimum number of fatalities and injuries resulting from terrorist attacks are zeros. In contrast, the September 11, 2001 attack caused a large number of killed and injured people, rising to the maximum of 1,380 and 10,878, respectively.

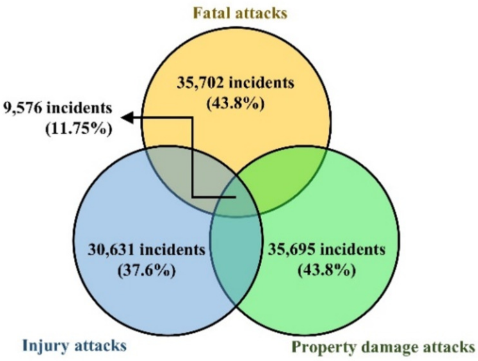

Fig.4: *Percentages of fatal, injury, and property damage attacks.*

Table 2: *Descriptive statistics of the number of fatalities and injuries from terrorist attacks.*

Statistics	Number of Fatalities	Number of Injuries
Average	1.46	2.80
SD	9.15	57.06
Minimum	0	0
Maximum	1,380	10,878

4.2 Selection of Machine Learning Models

To classify terrorist attacks, the top three ML models must be chosen for developing the level-1 classification models. In this experiment, seven ML models (i.e., KNN, LR, SVM, MLP, RF, GBM, and CatBoost) with default values of all hyperparameters were evaluated the performance in classifying fatal attacks, injury attacks, and property damage attacks. The average F1 scores and ranks of ML models according to their mean F1 scores, written in parentheses, are shown in Table 3.

In the classification of fatal attacks, the top three ML models were CatBoost, GBM, and RF, reaching the three highest mean F1 scores of 0.821, 0.817, and 0.808, respectively. In identifying injury attacks, CatBoost, GBM, and RF were the best three models with mean F1 scores of at least 0.695. In classifying property damage attacks, CatBoost, GBM, and RF achieved the top three mean F1 scores, which are 0.813, 0.809, and 0.802, respectively. Therefore, CatBoost, GBM, and RF were applied in the level-1 classification models to produce predicted scores of fatal, injury, and property damage attacks. These scores would be used as input features for the level-2 classification models to classify terrorist attacks. By grid search, the suitable hyperparameter settings of three base models (i.e., CatBoost, GBM, and RF) are obtained as shown in Table 4.

To choose regression models for predicting the number of fatalities and injuries, five ML models (i.e., RR, MLP, RF, GBM, and CatBoost) with the suitable hyperparameter values obtained from grid search were compared the average values of mean absolute

Table 3: *Average F1 scores and ranks of machine learning models.*

ML Models	Classification Types		
	Fatal Attacks	Injury Attacks	Property Damage Attacks
KNN	0.791 (6)	0.678 (5)	0.771 (7)
LR	0.792 (5)	0.653 (6)	0.781 (5)
SVM	0.791 (6)	0.646 (7)	0.782 (4)
MLP	0.798 (4)	0.692 (4)	0.778 (6)
RF	0.808 (3)	0.695 (3)	0.802 (3)
GBM	0.817 (2)	0.703 (2)	0.809 (2)
CatBoost	0.821 (1)	0.710 (1)	0.813 (1)

Table 4: *The hyperparameter settings of the base classifiers.*

Classifier	Model	Hyperparameter Setting
Fatal Attacks	CatBoost	$iterations = 2,000, learning\_rate = 0.1$
	GBM	$n\_estimators = 700, learning\_rate = 0.1$
	RF	$n\_estimators = 500$
Injury Attacks	CatBoost	$iterations = 2,500, learning\_rate = 0.1$
	GBM	$n\_estimators = 700, learning\_rate = 0.1$
	RF	$n\_estimators = 500$
Property Damage Attacks	CatBoost	$iterations = 2,000, learning\_rate = 0.15$
	GBM	$n\_estimators = 1,000, learning\_rate = 0.1$
	RF	$n\_estimators = 500$

errors (MAE) in predicting the number of fatalities and injuries, as shown in Figure 5. The lower MAE is better when comparing the performance of regression models.

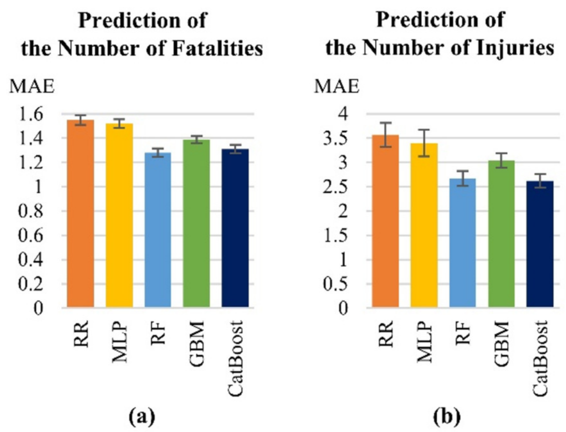

Fig.5: *MAEs of regression models in predicting the number of fatalities (a) and injuries (b).*

According to Figure 5 (a), RF outperformed the others in predicting the number of fatalities for fatal terrorist attacks with the lowest average MAE of 1.28. Thus, RF was used with a stacking ensemble classifier for predicting the number of killed civilians resulting from terrorist attacks. The suitable value of RF hyperparameter $n\_estimators$ gained from grid search is 300. From Figure 5 (b), CatBoost showed the lowest average MAE of 2.62 in predicting the number of injured people from terrorist attacks. Therefore, CatBoost was applied with a stacking ensemble classifier for predicting the number of injuries from terrorist attacks. The appropriate values of CatBoost hyperparameters *iterations* and *learning_rate* obtained from performing grid search are 2,000 and 0.15, respectively. The experimental results of hyperparameter tuning for the classification and regression models can be found in the supplementary information downloadable at `https://github.com/thitipongk/stacking-terrodamage`.

4.3 Performance of Stacking Ensemble Classifiers

In this section, the performance of the stacking ensemble classifiers proposed in this paper was evaluated and compared with a recently existing method (i.e., Hu's model [14]) in the classification of terrorist attacks regarding their consequent damage. The average values and SDs of performance measures of the proposed classification models are shown in Table 5. These stacking ensemble models were created based on the top three best classifiers, including CatBoost, GBM, and RF. The additional results of comparing different meta-models, or stacking ensemble models generated from combining different base classifiers, can be found in the supplementary information accessible at `https://github.com/thitipongk/stacking-terrodamage`.

Table 5: *Average values and SDs of performance measures of stacking ensemble classifiers.*

Performance Measures	Classification Types		
	Fatal Attacks	Injury Attacks	Property Damage Attacks
AUPR	0.904 ± 0.003	0.808 ± 0.008	0.910 ± 0.004
AUC	0.928 ± 0.003	0.881 ± 0.004	0.925 ± 0.004
PRE	0.813 ± 0.007	0.733 ± 0.007	0.828 ± 0.006
REC	0.850 ± 0.007	0.727 ± 0.013	0.818 ± 0.013
ACC	0.849 ± 0.005	0.798 ± 0.005	0.846 ± 0.006
MCC	0.695 ± 0.009	0.568 ± 0.010	0.686 ± 0.012
F1	0.831 ± 0.005	0.730 ± 0.006	0.823 ± 0.008

In the classification of fatal attacks, the stacking ensemble classifier reached high values of comprehensive performance measures, including a mean AUPR and AUC value of 0.904 and 0.928, respectively. Additionally, the proposed classifier could identify fatal attacks precisely with a mean accuracy and F1 score of 0.849 and 0.831, respectively. Similarly, the stacking ensemble models accurately classified terrorist attacks causing property damage with high average AUPR and AUC values of 0.910 and 0.925, respectively. In the classification of property damage attacks, the mean accuracy and F1 of the proposed classifier were 0.846 and 0.823, respectively.

In the classification of injury attacks, an average value of AUPR and AUC of the proposed model were 0.808 and 0.881, respectively. Moreover, the mean value of accuracy and F1 score were slightly dropped to 0.798 and 0.730, respectively, when compared to the values in the classification of fatal and property damage attacks. This may be because there is a higher imbalance ratio of the data used in the classification of injury attacks than those in the other classification types. The ratio of the number of injury attacks to the number of non-injury attacks is about 3:5 whereas the ratios of positives to negatives in the classification of fatal attacks and property damage attacks are about 4:5. With more imbalanced data sets, the ability of a classifier to distinguish between samples of minority (positive) class and majority (negative) class is decreased [27].

Next, the classification performance of the stacking ensemble classifiers was compared with that of Hu's model, an existing method recently introduced in 2022 [14]. Hu's model was created to classify casualty terrorist attacks, causing at least one death or injury, and predicting the number of deaths and injuries. To compare with Hu's model, the class labels of fatal and injury attacks were changed into casualty attacks if there was at least one death or injury reported and non-casualty attacks if there was not a death and an injury reported. The average and SD values of performance measures of Hu's model and the stacking ensemble models are shown in Table 6.

Table 6: *Comparison of classification performance with the existing method.*

Performance Measures	Hu's Model (2022)	Stacking Ensemble Models
AUPR	0.937 ± 0.002	0.958 ± 0.003
AUC	0.923 ± 0.003	0.950 ± 0.003
PRE	0.871 ± 0.003	0.906 ± 0.004
REC	0.892 ± 0.006	0.918 ± 0.007
ACC	0.855 ± 0.005	0.893 ± 0.003
MCC	0.696 ± 0.010	0.775 ± 0.007
F1	0.881 ± 0.004	0.912 ± 0.003

From the performance comparison in Table 6, it is noticeable that the stacking ensemble models outperformed Hu's model in the classification of casualty terrorist attacks with high average values of all evaluation metrics, particularly AUPR (0.958 ± 0.003), AUC (0.950 ± 0.003), PRE (0.906 ± 0.004), REC (0.918 ± 0.007), and F1 (0.912 ± 0.003). By performing paired t-tests, it was found that the proposed classifiers produced significantly higher average values of all performance measures at significance levels of below 1% (p-values $< 1 \times 10^{-7}$). According to the experimental results, it can be concluded that the stacking ensemble classification models can more accurately classify terrorist attacks than Hu's model. Furthermore, an advantage of the proposed method is that it can accurately predict property damage attacks whereas other existing methods focused on only casualty prediction.

4.4 Prediction Errors

In this section, the mean absolute errors (MAEs) of the proposed method in predicting the number of deaths and injuries were compared with those of Hu's model. The proposed method combines stacking ensemble classifiers with regression models to improve the accuracy of predictions of fatalities and injuries. To demonstrate the superior performance of the proposed method, ordinary regression models were used to compare with the proposed method. For forecasting the number of fatalities, RF was the best regression model with the lowest average MAE of 1.28. In predicting the number of injuries, CatBoost reached the lowest average MAE of 2.62. Then, CatBoost was chosen to compare with the proposed method. The average MAEs and SDs resulting from predicting the number of fatalities and injuries using different methods, including the proposed method, are shown in Table 7.

Table 7: *Comparison of mean absolute errors in predicting the number of fatalities and injuries.*

Prediction	Method		
	Hu's Model (2022)	**Best Regression Model**	**Proposed Method**
Number of Fatalities	1.52 ± 0.07	1.28 ± 0.07	1.22 ± 0.07
Number of Injuries	3.34 ± 0.45	2.62 ± 0.28	2.32 ± 0.28

From Table 7, it is noticeable that the proposed method showed the lowest average MAEs in predicting the number of fatalities (average MAE $= 1.22$) and injuries (average MAE $= 2.32$). By conducting paired t-tests, the proposed method significantly outperformed Hu's model in predicting the number of fatalities and injuries at significance levels below 1% (p-values $< 1 \times 10^{-4}$). Likewise, the proposed method more accurately predicted the number of deaths and injuries, resulting in significantly lower average MAEs than using the original regression models at significance levels of below 1% (p-values $< 1 \times 10^{-7}$).

When compared to the ordinary regression models, the superior performance of the proposed method could suggest that combining stacking ensemble classifiers with regression models can reduce the prediction errors of regression models, particularly in cases of non-fatal and non-injury attacks which typically were predicted with existing fatalities and injuries by the traditional regression models.

Although Hu's model utilized both classification and regression techniques resembling the proposed method, there are some differences between both methods possibly resulting in the superior performance of the proposed method. Firstly, using the stacking ensemble models to preliminarily separate between casualty and non-casualty attacks in the classification step could help reduce the prediction errors in finally estimating the number of fatalities and injuries. Secondly, using the data of multiple attack types, target types, and weapon subtypes in the proposed method could enhance prediction accuracy due to more information about terrorist attacks being retained and learned to predict the number of fatalities and injuries.

5. CONCLUSION

This paper proposed a stacking ensemble learning method with regression models for predicting damage from terrorist attacks. For classifying fatal, injury, and property damage terrorist attacks, RF, GBM, and CatBoost were chosen to incorporate with MLP to create the stacking ensemble models. In predicting casualty terrorist attacks, the proposed classifiers significantly outperformed Hu's model, a recent ML method, with an average AUPR and F1 of 0.958 and 0.912, respectively. An advantage of the proposed method is that it can accurately predict terrorist attacks causing property damage with an average AUPR and F1 of 0.910 and 0.823, respectively. By combining the stacking classifiers with regression models, the proposed method can substantially reduce the average MAEs to the lowest value of 1.22 in forecasting the number of fatalities and 2.32 in estimating the number of injuries. In conclusion, stacking ensemble learning with regression models is an efficient method for predicting damage from terrorist attacks, and it will be a promising tool to support decision-making in controlling and managing the emergency consequences of future terrorist incidents. Furthermore, the proposed models can be used to study further the crucial factors of terrorist attacks that influence consequential damage, which could be valuable information for planning actions against terrorism.

Despite the superior performance of the proposed method, one of its limitations is time and resource consumption in training three stacking ensemble classifiers to identify damage types of terrorist attacks independently. Additionally, the proposed models can classify property damage attacks but cannot estimate the levels of property damage. In the future, multi-label classification techniques can be applied to identify damage types of terrorist attacks simultaneously. Moreover, the prediction of property damage attacks can be enhanced to enable forecasting the levels of property damage by applying multiclass classification techniques. Additionally, deep learning (DL) models, such as convolution neural networks (CNN) and graph neural networks (GNN), can be used to develop a DL-based method to improve the prediction of damage from terrorist attacks.

ACKNOWLEDGEMENT

This work was supported by the Research Fund of Chulachomklao Royal Military Academy for 2023.

AUTHOR CONTRIBUTIONS

Conceptualization, T.K.; methodology, T.K.; data curation, T.K.; validation, T.K.; formal analysis, T.K.; writing—original draft preparation, T.K.; writing—review and editing, T.K.; funding acquisition, T.K. All authors have read and agreed to the published version of the manuscript.

References

[1] M. Helbling and D. Meierrieks, "Terrorism and Migration: An Overview," *British Journal of Political Science*, vol. 52, no. 2, pp. 977-996, 2022.

[2] G. LaFree and L. Dugan, "Introducing the Global Terrorism Database," *Terrorism and Political Violence*, vol. 19, no. 2, pp. 181-204, 2007.

[3] O. A. Olabanjo, B. S. Aribisala, M. Mazzara and A. S. Wusu, "An Ensemble Machine Learning Model for the Prediction of Danger Zones: Towards a Global Counter-Terrorism," *Soft Computing Letters*, vol. 3, pp. 1-6, 2021.

[4] M. I. Uddin *et al.*, "Prediction of Future Terrorist Activities Using Deep Neural Networks," *Complexity*, vol. 2020, pp. 1-16, 2020.

[5] F. Saidi and Z. Trabelsi, "A Hybrid Deep Learning-Based Framework for Future Terrorist Activities Modeling and Prediction," *Egyptian Informatics Journal*, vol. 23, no. 3, pp. 437-446, 2022.

[6] X. Pan and T. Zhang, "Machine Learning-Based Target Prediction for Terrorist Attacks," *Journal of Physics: Conference Series*, vol. 2577, no. 1, pp. 1-14, 2023.

[7] P. Agarwal, M. Sharma and S. Chandra, "Comparison of Machine Learning Approaches in the Prediction of Terrorist Attacks," *Proceedings of the 12th International Conference on Contemporary Computing (IC3)*, pp. 1-7, 2019.

[8] G. R. Ciottone, A. Hart, A. J. Hertelendy and D. Tin, "50 Years of Mass-Fatality Terrorist Attacks: A Retrospective Study of Target Demographics, Modalities, and Injury Patterns to Better Inform Future Counter-Terrorism Medicine Preparedness and Response," *Prehospital and Disaster Medicine*, vol. 36, no. 5, pp. 531-535, 2021.

[9] H. Xing, Z. Zhonglin and W. Shaoyu, "The Prediction Model of Earthquake Casualty Based on Robust Wavelet V-SVM," *Natural Hazards*, vol. 77, no. 2, pp. 717-732, 2015.

[10] B. Li, A. Gong, T. Zeng, W. Bao, C. Xu and Z. Huang, "A Zoning Earthquake Casualty Prediction Model Based on Machine Learning," *Remote Sensing*, vol. 14, no. 1, pp. 1-27, 2022.

[11] S. Sarkar, A. Pramanik, J. Maiti and G. Reniers, "Predicting and Analyzing Injury Severity: A Machine Learning-Based Approach Using Class-Imbalanced Proactive and Reactive Data," *Safety Science*, vol. 125, pp. 1-23, 2020.

[12] M. You, S. Li, D. Li and S. Xu, "Applications of Artificial Intelligence for Coal Mine Gas Risk Assessment," *Safety Science*, vol. 143, pp. 1-15, 2021.

[13] Y. Feng, D. Wang, Y. Yin, Z. Li and Z. Hu, "An XGBoost-Based Casualty Prediction Method for Terrorist Attacks," *Complex & Intelligent Systems*, vol. 6, no. 3, pp. 721-740, 2020.

[14] X. Hu, J. Hu and M. Hou, "A Two-Step Machine Learning Method for Casualty Prediction under Emergencies," *Journal of Safety Science and Resilience*, vol. 3, no. 3, pp. 243-251, 2022.

[15] L. Guohui, L. Song, C. Xudong, Y. Hui and Z. Heping, "Study on Correlation Factors that Influence Terrorist Attack Fatalities Using Global Terrorism Database," *Procedia Engineering*, vol. 84, pp. 698-707, 2014.

[16] Z. Li, X. Li, C. Dong, F. Guo, F. Zhang and Q. Zhang, "Quantitative Analysis of Global Terrorist Attacks Based on the Global Terrorism Database," *Sustainability*, vol. 13, no. 14, pp. 1-19, 2021.

[17] J. Yu, T. Xian, Z.-y. Hu and Y. Liu, "Hazard Grading Model of Terrorist Attack Based on Machine Learning," *International Journal of Advanced Network, Monitoring and Controls*, vol. 4, pp. 81-85, 2019.

[18] C.-Y. J. Peng, K. L. Lee and G. M. Ingersoll, "An Introduction to Logistic Regression Analysis and Reporting," *The Journal of Educational Research*, vol. 96, no. 1, pp. 3-14, 2002.

[19] T. Cover and P. Hart, "Nearest Neighbor Pattern Classification," *IEEE Transactions on Information Theory*, vol. 13, no. 1, pp. 21-27, 1967.

[20] C. Cortes and V. Vapnik, "Support-Vector Networks," *Machine Learning*, vol. 20, no. 3, pp. 273-297, 1995.

[21] F. Murtagh, "Multilayer Perceptrons for Classification and Regression," *Neurocomputing*, vol. 2, no. 5, pp. 183-197, 1991.

[22] L. Breiman, "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5-32, 2001.

[23] A. Natekin and A. Knoll, "Gradient Boosting Machines, A Tutorial," *Frontiers in Neurorobotics*, vol. 7, pp. 1-21, 2013.

[24] L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush and A. Gulin, "CatBoost: Unbiased Boosting with Categorical Features," *Proceedings of the 32nd International Conference on Neural Information Processing Systems*, pp. 6639–6649, 2018.

[25] W. Feng, J. Gou, Z. Fan and X. Chen, "An Ensemble Machine Learning Approach for Classification Tasks Using Feature Generation," *Connection Science*, vol. 35, no. 1, pp. 1-23, 2023.

[26] A. E. Hoerl and R. W. Kennard, "Ridge Regression: Biased Estimation for Nonorthogonal Problems," *Technometrics*, vol. 12, no. 1, pp. 55-67, 1970.

[27] M. Zheng, F. Wang, X. Hu, Y. Miao, H. Cao and M. Tang, "A Method for Analyzing the Performance Impact of Imbalanced Binary Data on Machine Learning Models," *Axioms*, vol. 11, no. 11, pp. 1-19, 2022.

Thitipong Kawichai accomplished his doctoral degree in applied mathematics and computational science from Chulalongkorn University, Thailand. He is currently an instructor at the Department of Mathematics and Computer Science, Academic Division, Chulachomklao Royal Military Academy, Thailand. His research interests encompass the development and application of computational methods based on machine learning and mathematical models in the bioinformatics and military domain.