Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105
Volume **11**, Number **1**, February **2026**

Design of New Energy Access Terminal Signature Authentication Method Based on Deep Discriminant Representation Learning

Wen-Di Chen[1,*], Mu-Xian Liu[1]

[1]Information Communication Branch of Guangxi Grid Company,
Nanning 530012, P. R. China
chenhui-vanter@foxmail.com, 852204098@qq.com

Zi-Jie Deng[2]

[2]CSG Digital Power Grid Group Co., Ltd.,
Guangzhou 510000, P. R. China
fmmmdxwd530937@qq.com

Zhi-Bo Dong[1], Gui-Hua Liu[1]

[1]Information Communication Branch of Guangxi Grid Company,
Nanning 530012, P. R. China
1730429667@qq.com, jingdada123@qq.com

[*]Corresponding author: Wen-Di Chen

Received October 22, 2024, revised February 07, 2025, accepted May 11, 2025.

Abstract. *Considering the security authentication needs of massive new energy terminals in the power system, this paper proposes a new energy access terminal signature authentication method based on deep discriminative representation learning in response to the problems of poor representation learning and low authentication efficiency of new energy terminal signature authentication methods in the power system. Firstly, the real terminal signature sequence and its synthesized samples are discriminatively processed relied on Generative Adversarial Network (GAN), and the GAN is guided to generate signature images with various key lengths based on the length condition of the signatures. Dynamic Time-Wise (DTW) distances are then used in the deep metric learning process to end-to-end optimize the distances between individual local positions of the signature sequences, thus facilitating the extraction of more discriminative signature features by the underlying network. Before the GAN-generated signatures are fed into the network, their time-functional features are extracted using CNN-GRU and signature elasticity matching is performed using DTW in the authentication phase, thus exploring more effective signature representations in the learning process. Finally, the DTW distance is compared with the preset threshold to obtain the final terminal signature authentication result. The experimental outcome implies that the offered approach has an authentication accuracy of 92.86% and an equal error rate of 1.57%, and the authentication efficiency is better than other methods, which can be better applied to the signature authentication of new energy terminals.*
Keywords: Deep discriminative representation learning; Terminal signature authentication; Generative adversarial network; CNN-GRU; Dynamic time regulation.

1. **Introduction.** New energy access terminals serve as an essential part of the power system and they are responsible for supplying power to end users [1]. Security authentication during the access phase of new energy terminal tasks can prevent unauthorized users or devices from accessing the power system [2]. If the new energy terminal requires frequent troubleshooting and maintenance, or has problems such as communication delays and data loss, it may adversely affect the normal operation of the entire power system. And security certification can ensure that the quality and performance of power terminals meet the standards, reduce the occurrence of faults and problems, and enhance the dependability and efficiency of the power system [3, 4]. In the practical application stage, the security authentication of new energy access terminals should be able to recognize and verify the identity of the user or device, and ensure that it has the correct authority. Thus, it holds immense practical importance for achieving efficient authentication of new energy access terminals.

1.1. **Related work.** The research of new energy access terminal security authentication method mainly focuses on signature authentication. Choi et al. [5] described the deficiencies of the security chip of power terminal and pointed out that it is necessary to build a lightweight signature verification system by combining hardware and software to realize distributed authorization of power terminal and high-speed security access authentication. Ren et al. [6] achieved endpoint signature authentication by optimizing the distance from the point to the set and using only real signatures. Fu et al. [7] obtained highly reliable endpoint signature samples by using top-rank learning to distance the positive samples from the most difficult negative samples as much as possible. Azhar et al. [8] manually extracted the features of signatures and achieved the authentication of terminal signatures by SVM. Wang et al. [9] used RankSVM based on ranking to replace SVM for terminal signature authentication, and achieved better authentication performance than SVM in the case of unbalanced data categories.

With the blowout progress of deep learning in various fields, the deep signature authentication technology of new energy access terminals has also been deeply developed. Xia et al. [10] added skillful forged signatures during the training of CNN, guided the model to carry out the multi-task learning of the authenticity dichotomy, and guided the network to extract the terminal signature features conducive to identity authentication. La et al. [11] introduced a spacing margin strategy for softmax-based linear classifiers, which optimizes the distance from the point to the set and achieves endpoint signature authentication when trained using only real signatures. Fan et al. [12] improved the performance of signature authentication by augmenting offline signatures at the image level and feature level based on Spatial Pyramid Pooling (SPP) and the intra-class variation of users' signatures.

Signature authentication methods based on deep learning have simpler tasks and looser constraints, and the learning effect is still not as good as desired, and more progressive discriminative representation learning methods need to be explored. Li et al. [13] applied twin networks to the terminal signature authentication task, but the authentication suffers from large delays. Parcham et al. [14] proposed a dual-channel CNN that, after aligning the grayscale images of the template signature and the signature to be tested, feeds them into the backbone network separately from different channels for discrimination. Tsotsopoulou et al. [15] learned a more efficient signature representation by inverting the branching structure and the attentional module of the discriminative network by grayscale. Jain et al. [16] used a simple twin structure based on a two-way recurrent neural network to achieve similar authentication accuracy as the twin network

on a publicly available dataset. Massaoudi et al. [17] also proposed a framework that combines reinforcement learning with Dynamic Time Warping (DTW) algorithm to further improve the generalization performance of the model.

To improve the generalization ability of the signature authentication model and to utilize a large amount of unlabeled signature data, Han et al. [18] introduced a generative adversarial network, which, after unsupervised training, uses the discriminator as a feature extractor. Zhang et al. [19] suggested a data enhancement approach relied on CycleGAN to obtain reconstructed signature images through generative adversarial learning and cyclic consistency learning, which can be used as augmentation data to improve the performance of signature authentication models.

1.2. **Contribution.** In summary, the existing new energy terminal signature authentication methods have insufficient samples and poor representation learning ability, leading to unsatisfactory authentication performance. For the goal of dealing with the above issues, this paper offers a new energy access terminal signature authentication method based on deep discriminative representation learning.

Firstly, GAN is introduced to discriminate the real terminal signature sequence and its synthesized samples to render the synthesized realistic signature images. Secondly, CNN-GRU is used to nonlinearly transform the input signature time function with context modeling to extract its time function features. Incorporating DTW distances into the deep metric learning process optimizes the distances between local positions in the signature sequence end-to-end, thus facilitating the extraction of more discriminative signature features by the underlying network. Signature elastic matching using DTW in the authentication phase to obtain all sequence-aligned paths in order to explore more efficient signature representations during the learning process. The DTW distance is compared with the preset threshold to obtain the final terminal signature authentication result. The experimental outcome implies that the suggested approach is with high authentication accuracy, low False Rejection Rate (FRR), False Acceptance Rate (FAR) and Equal Error Rate (EER), and can efficiently and accurately realize the signature authentication of new energy terminal.

2. **Theoretical analysis.**

2.1. **Deep discriminative representation learning theory.** Deep Discriminative Representation Learning utilizes inter-sample relations to supervise deep neural networks to learn nonlinear mappings from raw data, which are expected to yield features with strong discriminative properties [20]. It has been broadly adopted in computer vision tasks and also plays an irreplaceable role in other domains for example natural language understanding and speech recognition. The new energy access terminal signature authentication task performs identity authentication by comparing signature images, so the model is required to be able to capture the similarity between real signatures as well as the difference between genuine and fake signatures.

Deep Discriminative Representation Learning allows for multi-granularity similarity and dissimilarity comparisons and is an effective signature authentication scheme as shown in Figure 1, where feature extraction and classifier construction are merged into the same phase. The architecture contains two sub-networks with the same structure and shared weights, inputs signature pairs consisting of template signatures and to-be-tested signatures, and outputs normalized signature similarity scores.

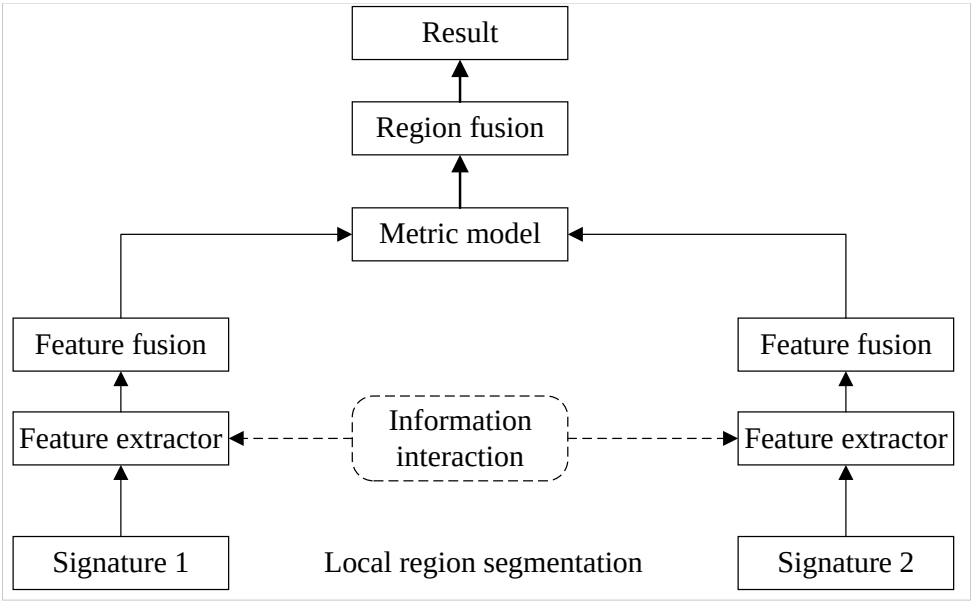

Figure 1. Deep discriminative learning process

2.2. **Convolutional neural network.** Unlike conventional machine learning methods, CNNs can study picture characteristics spontaneously without human intervention, which allows the network to automatically capture valuable characteristics from the data, improving the accuracy and universalization of the model. CNN is comprised of convolutional level, pooling level, fully connected level and nonlinear activation operation [21]. Assuming that the vector of input data is denoted as $x = (x_1, x_2, \ldots, x_{n-1}, x_n, cl)$, where $x_n \in R^d$ is the feature and $cl \in R$ denotes the class label, the convolutional layer contains multiple convolutional kernels W to perform convolutional operations on the input data to achieve the characteristic plane h, which produces a novel set of characteristics. The novel characteristic plane gained from a convolutional kernel W_l is as follows:

$$h_i^l = f(W_l * x_{i:i+l_c-1} + b_l) \tag{1}$$

where W_l is the weight, $b_l \in R$ is the bias term, f is the activation operation, and l_c is the window size. The convolution kernel is employed in all sets of characteristics to produce the characteristic plane $H = \{h_1^l, h_2^l, \ldots, h_{n-l_c+1}^l\}$, where $H \in R^{n-l_c+1}$. Next, a pooling operation is applied to each feature plane and new features are input to the fully connected level. The activation operation for the fully connected level is selected to be a softmax function as shown below:

$$\sigma_t = \text{softmax}(w_{ho}H + b_o) \tag{2}$$

The characteristic data processed by the CNN will be built into a novel characteristic plane vector Y.

2.3. **Generating adversarial network.** In GAN, generator G and discriminator D play against one another and outperform each other during adversarial training, optimizing their adversarial strategies with the help of each other's feedback [22], as indicated in Figure 2. G receives the random noise data z and generates the data $G(z)$, D gets the generated data $G(z)$ and the actual data x and distinguishes among the truth and falsity of this data, Real for true and Fake for false.

First initialize G and D, then input the random noise z into G. Perform the following steps during each round of training:

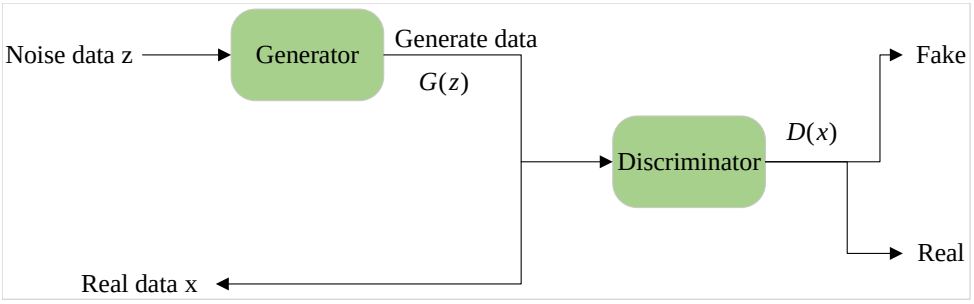

Figure 2. The structure of GAN

(1) Fix the parameters of G, train the parameters of D. Take a set of actual data X from the database, with forged data produced by G - and transfer it to D for training. Let it assign high scores to the actual data and low scores to the forged data.
(2) Fix the parameters of D and train the parameters of G. The false data produced by G is passed to D and assigned a score, and G is trained to make the assigned score higher. The core formula of GAN is as follows:

$$\min_G \max_D V(D,G) = E_{x\sim P_m}[\ln(D(x))] + E_{z\sim P_z}[\ln(1-D(G(z)))] \tag{3}$$

where $V(D,G)$ is the loss function, P_m is the distribution of the actual data, and P_z is the distribution of the produced data. Maximize $V(D,G)$ from the point of view of D, and then minimize $V(D,G)$ from the point of view of G. GAN obtains the near-optimal G by solving Equation (3).

3. **New energy access terminal signature image generation based on generative adversarial network.** Existing signature authentication methods for new energy access terminals face a serious challenge, namely, the lack of sufficient training data, and the collection, distribution, and commercial use of the signature data are prone to violating grid privacy. To deal with the above issues, in this paper, relied on GAN, the real terminal signature sequence and its synthesized samples are subjected to discriminative processing to generate realistic terminal signature images, so as to offer adequate training data for the signature authentication model. Second, to alleviate the problem that the terminal signature form is too homogeneous, the length condition based on the signature guides the GAN to generate signature images with diverse key lengths.

To convert the signature information of a new energy access terminal into a realistic signature Y, this paper defines the mapping $G : X \to Y$ and its inverse mapping $F : Y \to X$, where both G and F are learnable generators that can be trained simultaneously by means of adversarial learning [23]. Denote x as the instance from the origin domain X and y as the instance from the target domain Y. In addition to the generators G and F, the migration process involves the discriminators D_y and D_x. The migration process is characterized by the use of the following two parameters. G tries to generate signatures similar to the target sample, while D aims to correctly differentiate the generated signature from the real one. The adversarial loss of G and D_Y is computed as follows:

$$L_{G,GAN}(G, D_Y, X) = E_{x\sim P_{data}(x)}[(1 - D_Y(G(x)))^2] \tag{4}$$

$$L_{D_Y,GAN}(G, D_Y, X, Y) = 0.5\times E_{y\sim P_{data}(y)}[(1-D_Y(y))^2]+0.5\times E_{x\sim P_{data}(x)}[D_Y(G(x))^2] \tag{5}$$

The adversarial losses of F and D_x can be computed in a similar way by simply swapping the positions of X and Y and replacing G and D_y with F and D_x, individually.

Furthermore, to enhance the supervision of the G-learning process, the following cyclic consistency loss L_{cyc} and constant loss L_{idt} are imposed in this paper:

$$L_{cyc}(G,F) = E_{x\sim P_{data}(x)}[||F(G(x)) - x||_1] + E_{y\sim P_{data}(y)}[||G(F(y)) - y||_1] \tag{6}$$

$$L_{idt}(G,F) = E_{y\sim P_{data}(y)}[||G(y) - y||_1] + E_{x\sim P_{data}(x)}[||F(x) - x||_1] \tag{7}$$

where the L1 paradigm is adopted to compute the difference among the reconstructed image and the initial input image, L_{cyc} is used to motivate G to produce a picture that preserves the information of the original input content, and L_{idt} is used to motivate G to learn the constant mapping when fed actual instances of the target domain.

For the goal of improving the diversity of access terminal signature images, the signed key length control vector is used as a conditional input to generate diverse terminal signature images based on GAN. Assuming that the key length of the terminal signature is k, k is mapped to an n-dimensional vector z. Subsequently, z is fed into the hermitian space of G, which is jointly trained and updated with G. G learns on the target set $D_{tgt} = \{Y, z\}$ and instructs G to minimize the cross-entropy loss on its target set $D_{gen} = \{G(X), z\}$ after label smoothing:

$$L_{z,Gen}(G, D_Y, X) = -\sum_{(G(X),z)\in D_{gen}} (1-\varepsilon)\log p(z \mid D_Y(G(x))) - \sum_{(G(X),z)\in D_{gen}} \left[\frac{\varepsilon}{N-1}\sum_{z_i\in[1,N]} \log p(z_i \mid D_Y(G \tag{8}$$

$$L_{z,Dis}(D_Y, Y) = -\sum_{(y,z)\in D_{tgt}} (1-\varepsilon)\log p(z \mid D_Y(y)) - \sum_{(y,z)\in D_{tgt}} \left[\frac{\varepsilon}{N-1}\sum_{z_i\in[1,N]} \log p(z_i \mid D_Y(y))\right] \tag{9}$$

where $p(z \mid \cdot)$ is the probability of the z-th key length and ε controls the degree of label smoothing used for regularization. The overall loss functions of G and D after introducing the terminal signature key length condition vector are shown below:

$$L^*_{Gen}(G, F, D_X, D_Y) = L_{G,GAN}(G, D_Y, X) + L_{cyc}(G, F) + L_{idt}(G, F) + L_{z,Gen}(G, D_Y, X) \tag{10}$$

$$L^*_{Dis}(G, F, D_X, D_Y) = L_{D_Y,GAN}(G, D_Y, X, Y) + L_{z,Dis}(D_Y, Y) \tag{11}$$

Since the terminal signature lengths in practical scenarios are mainly concentrated in a limited range $[k_{down}, k_{up}]$, the key length labels assigned to G are also randomly selected from this range to ensure good generation results.

4. **Design of new energy access terminal signature authentication method based on deep discriminant representation learning.**

4.1. **CNN-GRU based signature sequence feature extraction for new energy access terminals.**

Focusing on the issue of poor characterization learning ability of existing new energy access terminal signature authentication methods, DTW distance [24] is incorporated into the double triad loss function used to learn discriminative characterization, and the distances between each local position of the signature sequences are optimized end-to-end through deep metric learning [25], so as to facilitate the extraction of more discriminative signature features by the underlying CNN. Before feeding the

GAN-generated signatures into the network, their time function features are extracted and signature elasticity matching is performed using DTW in the authentication phase to obtain all the sequence-aligned paths so as to explore more effective signature representations in the learning process. The structure of the proposed new energy access terminal signature authentication model is shown in Figure 3.

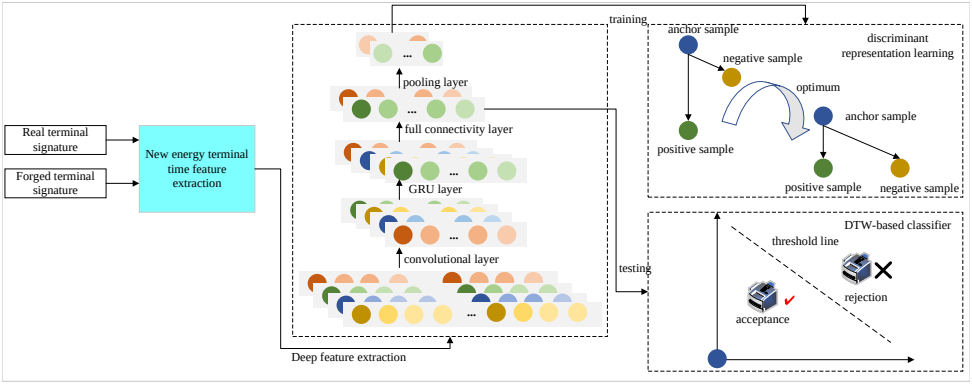

Figure 3. The proposed new energy access terminal signature authentication model

To fully extract the temporal features of the signature sequence of the new energy access terminal, this paper utilizes CNN and GRU for nonlinear transformation and context modeling of the input signature time function. The CNN-GRU consists of two one-dimensional convolution layers, a maximum pooling layer, an adaptive cycling layer of two GRU units, a linear layer, and an optional average pooling layer. According to the CNN feature extraction process in Section 2.2, it can be obtained that the terminal signature feature generated by GAN is h, the input at time t is h_t, and the output is o_t, and the GRU updates its output in the following way:

$$r_t = \text{sigmoid}(W_r \times h_t + U_r \times out_{t-1} + bias_r) \tag{12}$$

$$o_t = \tanh(W_o \times h_t + U_o \times (r_t \odot o_{t-1}) + bias_o) \tag{13}$$

where r_t is the reset gate, W_r, U_r, W_o, and U_o are the parameter matrix, $bias_r$ and $bias_o$ are the offset terms.

In general, the higher the time resolution of the signature sequence, the lower the authentication delay, but the memory consumption and computation increase in the square. When the length of the two input sequences is k_1 and k_2, the memory consumption and computation amount are both $O(k_1 k_2)$. Because the output sequence is too long, an optional averaging pooling layer is stacked in this paper, which only works in the training phase to double downsample the output signature sequence to reduce the video memory burden, and is removed in the test phase to improve the time resolution of the signature sequence and improve the signature authentication effect.

4.2. **Signature characterization of new energy access terminal based on DTW.** The new energy access terminal signature authentication task involves the distance between real and forged signatures, this paper adopts the idea of DTW to make the distance between real and forged signatures maximized and the distance between real signatures minimized. Considering the difference in the degree of forgery between skillful forged signatures and random forged signatures, this paper introduces Dual Triplet Loss to obtain a more discriminative signature characterization. The term "Dual" refers to setting different spacing margins for signatures with different levels of forgery.

First, calculate the DTW distance of the signature pair. $X = [x_1, x_2, \ldots, x_{k_1}] \in R^{d\times k_1}$ and $Y = [y_1, y_2, \ldots, y_{k_2}] \in R^{d\times k_2}$ are defined as two signature feature sequences of length k_1 and k_2 extracted by CNN-GRU, x_i and y_i are local feature vectors of d dimension, and the loss matrix between sequence X and Y is $\Delta(X,Y) \in R^{k_1\times k_2}$, where $[\Delta(X,Y)]_{i,j} = ||x_i - y_i||_2^2$. Let $\chi_{k_1\times k_2} \subset \{0,1\}^{k_1\times k_2}$ be the set of feasible two-valued alignment matrices, and $A \in \chi_{k_1\times k_2}$ satisfies the boundary condition $[A]_{1\times 1} = [A]_{k_1\times k_2} = 1$ and have both monotonicity and increment. Then the DTW distance of the signature sequence for X and Y is as follows:

$$DTW_\gamma(X,Y) = \min{}^\gamma\{\langle A, \Delta(X,Y)\rangle, A \in \chi_{k,m}\} \tag{14}$$

where $\langle A, \Delta(X,Y)\rangle$ is the inner product of A and $\Delta(X,Y)$, min^γ is the generalized min operator with a smoothing parameter defined as follows:

$$\min{}^\gamma a_1, \ldots, a_n = \begin{cases} \min_{i=1,\ldots,n} a_i \\ -\gamma \log \sum_{i=1}^n e^{-a_i/\gamma} \end{cases} \tag{15}$$

For the signature sequence pair X and Y, the following DTW-based distance is used in the training phase:

$$d_{train}(X,Y) = \frac{DTW_\gamma(f(X), f(Y))}{|f(X)| + |f(Y)|} \tag{16}$$

where $|\cdot|$ is the length of the input sequence.

The DTW distance of the signature pair is incorporated into the triplet loss function [26]. Each data batch samples n_u different terminals, and the l terminal collects 1 real signature X_a^l, n_g remaining real signatures $\{X_{g,i}^l, i = 1, \ldots, n_g\}$ and n_f forged signatures, which serve as anchor samples, positive samples and negative samples respectively. There are $n_g \times n_f$ triples for each user. The $n_f = n_{f,s} + n_{f,r}$ negative samples include $n_{f,s}$ skilled forged signatures $X_{f,s,j}^l$ and $n_{f,r}$ random forged signatures $X_{f,r,j}^l$. The DTW distance is incorporated into the double triplet loss function for the L-th user, and different interval margins are set for skilled and random forged signatures, m_1 and m_2, respectively. For the l-th terminal, denote the ternary losses of the negative samples filled with skillfully forged signatures and randomly forged signatures as $loss_{l,s}$ and $loss_{l,r}$, respectively, as follows:

$$loss_{l,s} = \frac{\sum_{i=1}^{n_g}\sum_{j=1}^{n_{f,s}} ReLU(d_{train}(X_a^l, X_{g,i}^l) + m_1 - d_{train}(X_a^l, X_{f,s,j}^l))}{1 + \sum_{i=1}^{n_g}\sum_{j=1}^{n_{f,s}} \Pi\{ReLU(d_{train}(X_a^l, X_{g,i}^l) + m_1 - d_{train}(X_a^l, X_{f,s,j}^l)) > 0\}} \tag{17}$$

$$loss_{l,r} = \frac{\sum_{i=1}^{n_g}\sum_{j=1}^{n_{f,r}} ReLU(d_{train}(X_a^l, X_{g,i}^l) + m_2 - d_{train}(X_a^l, X_{f,r,j}^l))}{1 + \sum_{i=1}^{n_g}\sum_{j=1}^{n_{f,r}} \Pi\{ReLU(d_{train}(X_a^l, X_{g,i}^l) + m_2 - d_{train}(X_a^l, X_{f,r,j}^l)) > 0\}} \tag{18}$$

where $l = 1, 2, \ldots, n_u$. In order to bring individual real signatures closer to each other, the loss $loss_{l,g}$ of intra-class differences in real signatures is considered, calculated as follows:

$$loss_{l,g} = \frac{1}{n_g}\sum_{i=1}^{n_g} d_{train}(X_a^l, X_{g,i}^l) \tag{19}$$

Then the overall loss function used to train the CNN-GRU is as follows:

$$loss_{total} = \frac{1}{n_u}\sum_{k=1}^{n_u}(loss_{l,s} + loss_{l,r} + \lambda loss_{l,g}) \tag{20}$$

where the hyperparameter λ is used to control the weight of the intra-class difference loss term. Since this paper incorporates the DTW distance into the dual triad loss function, the whole model can be successfully trained from end to end, so as to induce the underlying network to learn the deep signature characterization of new energy access terminals that is more conducive to identification.

4.3. **New energy access terminal signature authentication based on deep discriminative representation learning.** In the authentication phase, for the signature sequence Y to be authenticated and the template signature X of the claimed identity, the features $f'(Y)$ and $f'(X)$ are extracted using the trained CNN-GRU, then the dynamic time-regularized distance of the signature sequence in the feature space based on dynamic time regularization is as follows:

$$d_{test}(X,Y) = \frac{DTW(f'(X), f'(Y))}{|f'(X)| + |f'(Y)|} \tag{21}$$

where $DTW(f'(X), f'(Y))$ is the dynamic time-regularized distance between two sequences, calculated as follows:

$$DTW(f'(X), f'(Y)) = \min_{A \in \chi_{f'(X),f'(Y)}} \langle A, \Delta(f'(X), f'(Y)) \rangle \tag{22}$$

To obtain better overall authentication performance of the terminal, this paper uses a linear classifier based on normalized distance [27] for the final signature authentication decision. Denote $\{X_i^l, i = 1, \ldots, N\}$ as the N template signature of terminal l with intraclass distance $\bar{d}_{tmp}^l$. If there is only one template signature, set $\bar{d}_{tmp}^l = 1$. For signature Y to be tested, which claims to be terminal l, the normalized minimum and average distances are calculated as follows:

$$d_{min}^l(Y) = \frac{1}{N}\sum_{i=1}^{N} d_{test}(X_i^l, Y)/\bar{d}_{tmp}^l \tag{23}$$

$$d_{avg}^l(Y) = \min_{i=1,\ldots,N} d_{test}(X_i^l, Y)/\bar{d}_{tmp}^l \tag{24}$$

After comparing the calculated distance with the preset threshold θ, the final signature authentication result can be obtained. If $d_{min}^l(Y) + d_{avg}^l(Y) < \theta$, signature Y is accepted as the true signature of terminal l, otherwise it is regarded as a forged signature.

5. Experiment and result analysis.

5.1. **Authentication result analysis.** To evaluate the performance of the designed new energy access terminal signature authentication method, this paper uses the new energy terminal signatures of the power system from the literature [28] as the experimental dataset, which contains a total of 934 signature records from 186 terminals. This paper utilizes the open source software radio platform to establish the terminal nodes and use Matlab for signature authentication performance analysis. The experimental processor is Intel Xeon CPU E5-1620 3.50 GHz with 16G of RAM and NVIDIA Quadro K1200 graphics card. The number of training rounds in the experiment is 3000, the batch size is 16 and the learning rate is 0.01.

Under the above test environment, the ratio (R) of the training set to the test set is varied, respectively, and the signature authentication method (OURS) designed in this paper is analyzed and compared with the SPP_CNN method in the literature [12], the DPB_CNN method in the literature [14], and the RL_DTW method in the literature [17]. The ratio of the variable training set to the test set is set to 9:1, 8:2 and 3:7 respectively, and the authentication time and accuracy test results under the three methods are obtained as shown in Figure 4.

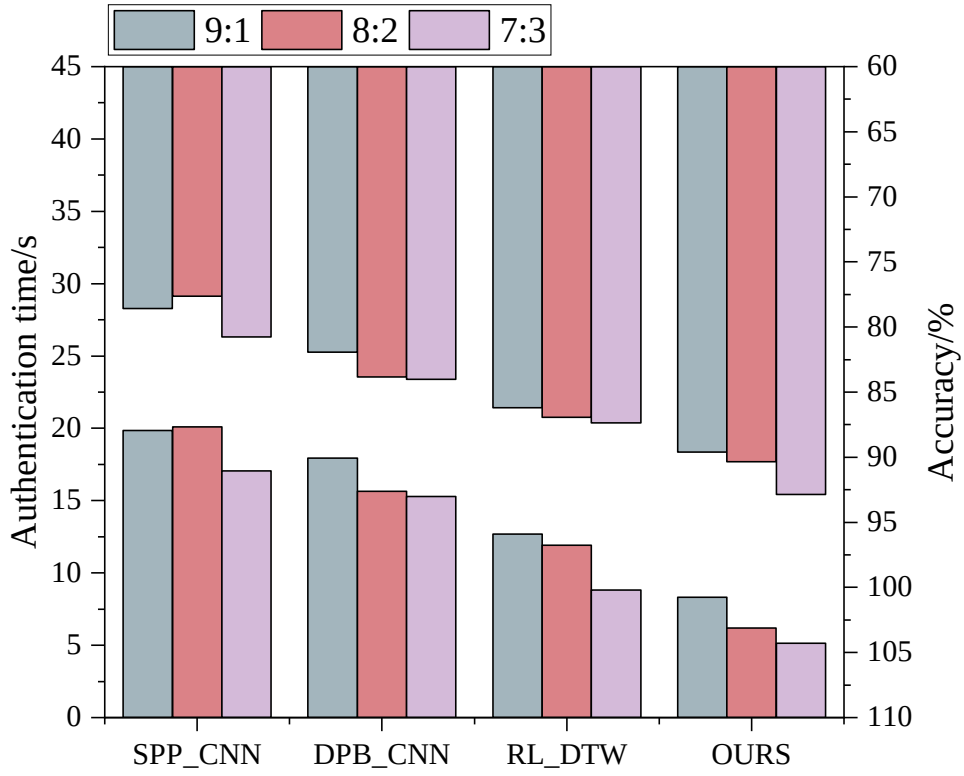

Figure 4. Authentication time and accuracy test results

When the ratio of the training set to the test set is 9:1, the authentication of OURS consumes the least amount of time and has the highest authentication accuracy. On the basis of using CNN for signature feature extraction, deep discriminative representation learning is used to make a further distinction between the features of the signature, which reduces the authentication time and ensures the authentication accuracy. When the ratio of training set to test set is 8:2 and 7:3, with the decrease of the number of training set and the increase of test set, the authentication time in this paper's method decreases, the test time increases slightly, and the authentication accuracy improves, which is obviously better than the other three methods.

In addition, the probability of the terminal being successfully attacked under different numbers of authenticated terminals is used as an evaluation index. In particular, when the number of authenticated terminals for attack control is set to 5, 10, 15, ..., 50, the corresponding test results are shown in Figure 5. As the amount of attack control authentication nodes increases, the probability of successful attack shows a steady increase. When the amount of attack control authentication nodes reaches 30, the probability of successful attacks on SPP_CNN, DPB_CNN, and RL_DTW are 0.125%, 0.098%, and 0.079%, respectively, implying that there is room for further optimization of the defense capability against large-range attacks. In contrast, in the test results of OURS method,

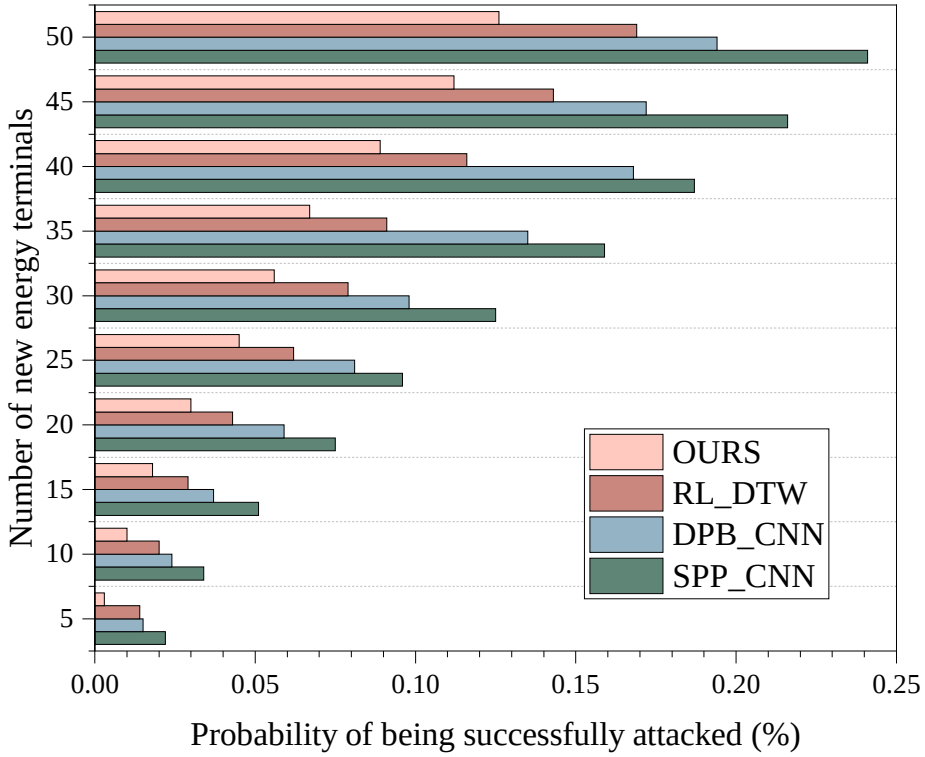

Figure 5. Comparison of attack success probability

the possibility of successful attack also exists when the number of attack-controlled authentication nodes reaches 10, but the corresponding probability is only 0.01%, which is essentially lower than that of the comparison method, and not only that, when the amount of attack-controlled authentication nodes reaches 30, the probability of successful attack is only 0.056%, which is lower than that of the other three methods, thus verifying the validity of OURS.

5.2. **Authentication performance analysis.** To further measure the authentication performance of OURS methods, the evaluation metrics of FRR, FAR and EER [29], which are commonly used to evaluate the terminal signature authentication algorithms, are introduced to analyze the authentication performance of the various methods, as shown in Table 1. The FRR, FAR, and EER of OURS are 2.69%, 1.31%, and 1.57%, respectively, which are 5.45%, 4.01%, and 6.36% lower compared to SPP_CNN, 2.63%, 2.47%, and 3.32% lower compared to DPB_CNN, and 2.27%, 1.3%, and 2.27%, 1.3%, and 2.27%, 1.3%, and 1.68%, respectively, compared to RL_DTW, 1.68%.

Table 1. Comparison of signature authentication performance of different terminals

Method	**FRR (%)**	**FAR (%)**	**EER (%)**
SPP_CNN	8.14	5.32	7.93
DPB_CNN	5.32	3.78	4.89
RL_DTW	4.96	2.61	3.25
OURS	**2.69**	**1.31**	**1.57**

Although SPP_CNN solves the problem that CNN needs fixed input size by utilizing SPP, the computation is large, which affects the speed of terminal signature authentication. DPB_CNN performs feature extraction and discrimination on the grayscale images of the aligned template signatures and the signatures to be tested by means of two-channel CNN, but it requires a more complex network structure and larger computational resources, which will increase the complexity of the model and the training cost. RL_DTW extracts the feature sequence of terminal signature through DNN and judges the distance between the sequences through DTW to decide the authenticity of the signature, but it does not consider the time information of the signature feature sequence, so the authentication performance is not as good as OURS.

6. **Conclusion.** Intending to the existing new energy terminal signature authentication method with poor representation learning ability and unsatisfactory authentication performance, this paper proposes a new energy access terminal signature authentication method based on deep discriminative representation learning. Firstly, GAN is introduced to discriminate the real terminal signature sequence and its synthesized samples to render and synthesize realistic signature images, based on which, GAN is guided to generate signature images with various key lengths based on the length conditions of the signatures. The CNN-GRU is adopted to capture the temporal function characteristics of the input signature by nonlinear transformation and context modeling. The DTW distance is used in the deep metric learning process to optimize the distances between local positions of the signature sequences end-to-end, thus facilitating the CNN-GRU to extract more discriminative signature features. In the authentication phase, DTW is used for signature elasticity matching, and the final terminal signature authentication result is obtained by comparing the DTW distance with the preset threshold. The experimental outcome indicates that the suggested method has high authentication accuracy, low attack success probability, and effectively improves the efficiency of terminal signature authentication.

REFERENCES

[1] J. Nan, W. Yao, and J. Wen, "Energy storage-based control of multi-terminal DC grid to eliminate the fluctuations of renewable energy," *The Journal of Engineering*, vol. 26, no. 16, pp. 991-995, 2019.

[2] Ç. Iris, and J. S. L. Lam, "A review of energy efficiency in ports: Operational strategies, technologies and energy management systems," *Renewable and Sustainable Energy Reviews*, vol. 112, pp. 170-182, 2019.

[3] U. Jassmann, A. Frehn, H. Röttgers, F. Santjer, C. Mehler, T. Beißel, L. Kaven, D. von den Hoff, R. Frühmann, and S. Azarian, "CertBench: Conclusions from the comparison of certification results derived on system test benches and in the field," *Forschung Im Ingenieurwesen*, vol. 85, no. 2, pp. 353-371, 2021.

[4] R. Gao, and J. Jiang, "Design and implementation of environmental design based on new energy technology," *Energy Reports*, vol. 8, pp. 7600-7611, 2022.

[5] B.-G. Choi, E. Jeong, and S.-W. Kim, "Multiple security certification system between blockchain based terminal and internet of things device: Implication for open innovation," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 5, no. 4, 87, 2019.

[6] S. Ren, D. Chen, Y. Tao, S. Xu, G. Wang, and Z. Yang, "Intelligent terminal security technology of power grid sensing layer based upon information entropy data mining," *Journal of Intelligent Systems*, vol. 31, no. 1, pp. 817-834, 2022.

[7] Q. Fu, Z. Ang, L. Yi, P. Xu, J. Liu, Z. Liang, L. Fu, C. Yang, and G. Fan, "A new terminal and electric meter legality authentication method," *Journal of Computers*, vol. 32, no. 6, pp. 176-182, 2021.

[8] N. A. Azhar, N. A. Mohamed Radzi, K. H. Mohd Azmi, F. S. Samidi, and A. Muhammad Zainal, "Criteria selection using machine learning (ML) for communication technology solution of electrical distribution substations," *Applied Sciences*, vol. 12, no. 8, 3878, 2022.

[9] Y. Wang, J. e. Li, X. Chen, H. Lin, F. Yu, and J. Luo, "Remote attestation for intelligent electronic devices in smart grid based on trusted level measurement," *Chinese Journal of Electronics*, vol. 29, no. 3, pp. 437-446, 2020.

[10] Z. Xia, D. Yin, K. Gu, and X. Li, "Privacy-Preserving Electricity Data Classification Scheme Based on CNN Model with Fully Homomorphism," *IEEE Transactions on Sustainable Computing*, vol. 8, no. 4, pp. 652-669, 2023.

[11] Y. La, J. Zhao, and W. Zhang, "Security authentication scheme for power terminals based on the SM9 threshold signature," *Journal of Electric Power Science and Technology*, vol. 37, no. 4, pp. 183-188, 2022.

[12] C. Fan, H. Gong, M. Cheng, B. Ye, L. Deng, Q. Yang, and D. Liu, "Identify the device fingerprint of OFDM-PONs with a noise-model-assisted CNN for enhancing security," *IEEE Photonics Journal*, vol. 13, no. 4, pp. 1-4, 2021.

[13] J. Li, R. Liu, H. Lin, S. Ye, M. Ye, X. Wang, and X. Zhu, "Tensor Network-Encrypted Physical Anti-counterfeiting Passport for Digital Twin Authentication," *ACS Applied Materials & Interfaces*, vol. 13, no. 51, pp. 61536-61543, 2021.

[14] E. Parcham, M. Ilbeygi, and M. Amini, "CBCapsNet: A novel writer-independent offline signature verification model using a CNN-based architecture and capsule neural networks," *Expert Systems with Applications*, vol. 185, 115649, 2021.

[15] E. Tsotsopoulou, X. Karagiannis, T. Papadopoulos, A. Chrysochos, A. Dyśko, and D. Tzelepis, "Protection scheme for multi-terminal HVDC system with superconducting cables based on artificial intelligence algorithms," *International Journal of Electrical Power & Energy Systems*, vol. 149, 109037, 2023.

[16] H. Jain, M. Kumar, and A. M. Joshi, "Intelligent energy cyber physical systems (iECPS) for reliable smart grid against energy theft and false data injection," *Electrical Engineering*, vol. 104, no. 1, pp. 331-346, 2022.

[17] M. S. Massaoudi, H. Abu-Rub, and A. Ghrayeb, "Navigating the landscape of deep reinforcement learning for power system stability control: A review," *IEEE Access*, vol. 11, pp. 134298-134317, 2023.

[18] K. Han, K. Yang, and L. Yin, "Lightweight actor-critic generative adversarial networks for real-time smart generation control of microgrids," *Applied Energy*, vol. 317, pp. 119163, 2022.

[19] Z. Zhang, K. Zuo, R. Deng, F. Teng, and M. Sun, "Cybersecurity analysis of data-driven power system stability assessment," *IEEE Internet of Things Journal*, vol. 10, no. 17, pp. 15723-15735, 2023.

[20] X. Jia, X.-Y. Jing, X. Zhu, S. Chen, B. Du, Z. Cai, Z. He, and D. Yue, "Semi-supervised multi-view deep discriminant representation learning," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 43, no. 7, pp. 2496-2509, 2020.

[21] Z. Li, F. Liu, W. Yang, S. Peng, and J. Zhou, "A survey of convolutional neural networks: analysis, applications, and prospects," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 12, pp. 6999-7019, 2021.

[22] C. Wang, C. Xu, X. Yao, and D. Tao, "Evolutionary generative adversarial networks," *IEEE Transactions on Evolutionary Computation*, vol. 23, no. 6, pp. 921-934, 2019.

[23] L.-A. Sutherland, and F. Marchand, "On-farm demonstration: enabling peer-to-peer learning," *Taylor & Francis*, vol. 5, pp. 573-590, 2021.

[24] T.-Y. Wu, H. Li, S. Kumari, and C.-M. Chen, "A Spectral Convolutional Neural Network Model Based on Adaptive Fick's Law for Hyperspectral Image Classification," *Computers, Materials & Continua*, vol. 79, no. 1, pp. 19-46, 2024.

[25] J. Lu, J. Hu, and Y.-P. Tan, "Discriminative deep metric learning for face and kinship verification," *IEEE Transactions on Image Processing*, vol. 26, no. 9, pp. 4269-4282, 2017.

[26] W. Min, S. Mei, Z. Li, and S. Jiang, "A two-stage triplet network training framework for image retrieval," *IEEE Transactions on Multimedia*, vol. 22, no. 12, pp. 3128-3138, 2020.

[27] C. Vivaracho-Pascual, M. Faundez-Zanuy, and J. M. Pascual, "An efficient low cost approach for on-line signature recognition based on length normalization and fractional distances," *Pattern Recognition*, vol. 42, no. 1, pp. 183-193, 2009.

[28] Y. Yang, L. Wu, C. Wang, and H. Ai, "Research on security access and authentication technology of power terminal based on TNC," *Applied Mechanics and Materials*, vol. 494, pp. 1623-1626, 2014.

[29] S. Ayeswarya, and J. Norman, "A survey on different continuous authentication systems," *International Journal of Biometrics*, vol. 11, no. 1, pp. 67-99, 2019.