Research on the Application of Convolutional Neural Network Based Image Encryption Technology in Behavioral Monitoring of Prisoners Serving Sentences

Fei Gao[1,*]

[1] Department of Information Technology, Henan Judicial Police Vocational College, Zhengzhou, Henan, 450046, China

Corresponding authors: (e-mail: Gaofeifeii0@163.com).

Abstract Prison management faces the problem of monitoring the behavior of incarcerated people, and the traditional monitoring methods have defects such as poor real-time performance and low confidentiality. This study proposes a behavioral monitoring method for prison inmates based on convolutional neural network image encryption technology. This method extracts the original features of the image, uses a filter for filter diffusion processing, combines convolutional neural network and compression perception theory to generate image hybrid phase mask, and finally realizes image encryption protection by replacing the image hybrid phase mask. The experiment adopts the self-constructed prison behavior dataset of inmates, which contains a total of 710 video samples of abnormal behaviors such as fighting, attacking the police, falling down and other daily behaviors. The results show that the proposed model has an accuracy of 94.14% in the assessment of the risk of assault, which is higher than 91.10% and 91.16% for the risk of suicide and the risk of negative rehabilitation. When the number of graph convolution layers is 2, the model performance is optimal with AUC value, accuracy, recall and F1 value of 96.26%, 92.17%, 88.25% and 85.72%, respectively. The analysis by manual intervention shows that the abnormal behaviors of prison inmates with appropriate intervention are significantly alleviated, while the non-interventionists still maintain the high sensitivity score status. The results of image encryption processing show that the pixel values of the ciphertext image are close to uniform distribution in the 0-255 interval, which effectively hides the statistical features of the plaintext image and ensures the security of the monitoring data. This study provides technical support for intelligent management and risk prevention and control in prisons, and has practical value for improving the modernized management level of prisons.

Index Terms convolutional neural network, image encryption, behavioral monitoring, prison management, risk assessment

I. Introduction

Prison is a penal enforcement unit in China, mainly responsible for the punishment, reform and custody of sentenced persons, and the efficient fulfillment of these missions is crucial for the long-term stability of the country and society [1]. Accompanied by reform and opening up, the state attaches more and more importance to the construction of the rule of law, and the security system of prisons has gradually developed from the traditional physical defense to modern intelligent management [2]. The need to apply artificial intelligence and other technologies to the prison video monitoring system to make it more efficient to complete the supervision of the inmates and minimize the investment of financial and human resources has become more and more urgent [3]-[5].

Prisoners in prison life has a strict regularity of life, and their daily activities and behaviors roughly form a fixed pattern [6]. If some inmates show abnormal behavior in a period of time, such as staying for a long time in some previously unseen locations, gathering and communicating abnormally in a certain area, and deliberately contacting with new people, these abnormal behaviors in the activity pattern are not easy to be detected by the prison guards [7]-[10]. By introducing a monitoring system supported by intelligent algorithms, it can intuitively output a series of information about the activity patterns of the inmates and reminders of abnormal information, which greatly reduces the workload of the prison guards [11], [12]. For this reason, the research on deep learning-based monitoring system is carried out, which enables the model to successfully and automatically detect and identify specific abnormal behaviors in prisons by characterizing the specific behaviors of the targets in a specific place and combining them with the learning of higher-dimensional features [13]-[16].

In recent years, behavioral monitoring of prison inmates has become an important topic in the field of public safety. In the prison environment, abnormal behaviors of inmates such as fighting, assaulting police, and suicide not only threaten the internal order of the prison, but also may lead to serious personal safety problems. Traditional

monitoring methods mainly rely on manual patrol and fixed camera monitoring, which has problems such as large monitoring blind spot, poor real-time, low efficiency of monitoring data processing, and insufficient security. Especially in the process of data transmission and storage, the surveillance video may be illegally accessed or tampered with, leading to the leakage of important information. Therefore, it is of great significance to develop an efficient and secure behavioral monitoring system for prison inmates. Convolutional neural network (CNN), as an important technology in the field of deep learning, performs well in image recognition and video analysis, and is able to effectively extract image features and identify the behavior of people in complex scenes. Meanwhile, image encryption technology can ensure the security of surveillance data during transmission and storage by encrypting video image data. Combining convolutional neural network and image encryption technology to build a safe and efficient behavioral monitoring system for prison inmates has become a current research hotspot. Existing researches mostly focus on single technology applications, such as only using neural networks for behavior recognition, or only using conventional encryption methods to protect image data, lacking comprehensive solutions. In addition, most of the studies use public datasets for experiments, which have complex backgrounds and differ greatly from the actual prison scenes, making it difficult to accurately reflect the behavioral characteristics in real prison environments. Behavioral monitoring of prison inmates not only needs to achieve behavioral recognition, but also needs to predict potential risks and ensure data security, which puts higher requirements on the technology.

In this study, we propose a behavioral monitoring method for prison inmates that combines convolutional neural network and image encryption technology. First, a multi-layer convolutional neural network structure is designed to extract image features and perform behavior recognition; second, an image encryption scheme is designed based on the theory of compressed perception, including four steps of extracting the original features of the image, filtering and diffusion processing, generating a mixed-phase mask, and replacing the mixed-phase mask, to achieve encrypted protection of the monitoring image; lastly, a behavioral risk assessment model of incarcerated people is established, and a self-constructed prison behavioral dataset for experimental verification. This research realizes the intelligent identification, security encryption and risk warning of the behavior of incarcerated people through technology integration, provides technical support for prison management, and is of great value for improving the level of prison management and preventing security risks.

II. Image encryption based on convolutional neural networks

II. A. Neural Networks

II. A. 1) Forward propagation

Figure 1 shows the neuron structure, forward propagation is the process of utilizing a neural network so that the input data x_i is processed by weights w, offsets b and activation function f and thus the output result is obtained [17]. The basic unit of a neural network is the neuron model.
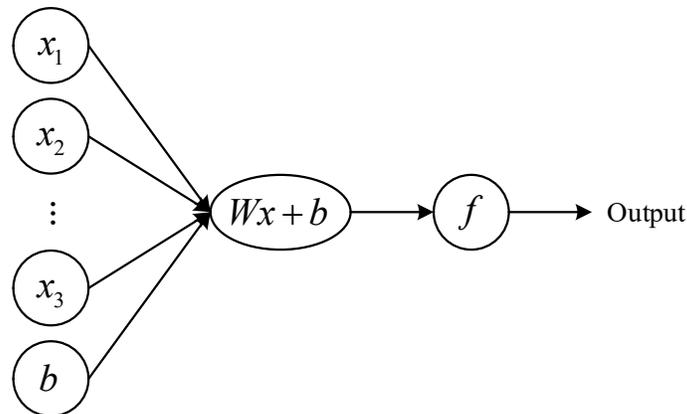

Figure 1: Neuron structure

A fully connected network of multiple neurons is shown in Figure 2.
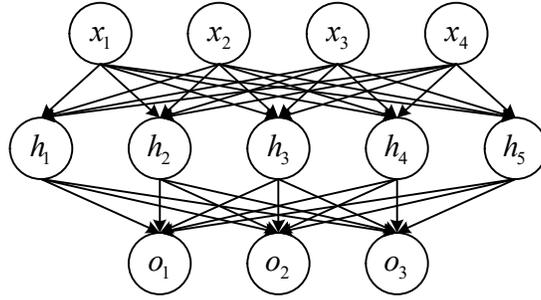
Figure 2: Three-layer fully connected network structure

The output value of each node in the output layer of the graph is calculated as follows:

$$O = W_o \cdot (W_h \cdot X + b_h) + b_o = W_o W_h X + W_o b_h + b_o \tag{1}$$

where X is the input, O is the output of the output layer, and W_h, b_h, W_o and b_o are the weights and bias parameters of the hidden and output layers, respectively.

II. A. 2) **Activation function**

Introducing an activation function in a fully connected network can change the linear structure of the network, allowing it to solve more complex problems. Common activation functions include Sigmoid function and Tanh function in saturated activation function and ReLU function and Leaky ReLU function in unsaturated function. In this section, the Sigmoid function and ReLU function are introduced.

(1) Sigmoid function

The structure of the Sigmoid function is relatively simple, and its calculation formula is as follows:

$$Sigmoid(x) = \frac{1}{1 + e^{-x}} \tag{2}$$

As can be learned from Eq. Soft saturation causes the input to this function to converge to infinity when the derivative there tends to zero, resulting in a vanishing gradient that further hinders the backpropagation process.

(2) ReLU function

The calculation of the ReLU activation function is relatively simple, and its formula is as follows [18]:

$$ReLU(x) = \max(0, x) \tag{3}$$

II. A. 3) **Reverse propagation**

The process of using the gradient descent optimization algorithm to update the weight parameters in the regulation model and adjust the error of the objective function to the desired range after several iterations of comparison to train the target network is the back propagation algorithm. The specific process of the algorithm is as follows:

(1) Input raw data in the input layer of the neural network

(2) Set the initial network parameters to random values close to 0 and set the learning rate α to an appropriate value

(3) Let the input data be I, and the output data be O

(4) Let δ^n be the difference between the desired data o^j and the actual data t^n, and calculate its specific value by the following two equations:

$$\delta^n = (t^n - o^j) t^n (1 - o^j) \tag{4}$$

$$\delta^m = h^j (1 - h^j) \sum w^{j+1} \delta^n \tag{5}$$

(5) The weight parameters are updated by the following four equations:

$$w_{km}^j(r+1) = w_{km}^j(r) + \Delta w_{km}^j(r) \tag{6}$$

$$w^{j+1}(r+1) = w^{j+1}(r) + \Delta w^{j+1}(r) \tag{7}$$

$$b^j(r+1) = b^j(r) + \Delta b^j(r) \tag{8}$$

$$d^{j}(r+1) = d^{l}(r) + \Delta d^{l}(r) \tag{9}$$

(6) Retain the adjusted parameters.

II. B. Two-dimensional convolutional neural networks

II. B. 1) Basic principles

In this subsection, several network layers of 2D convolutional neural networks are briefly described.

(1) Input layer

Depending on the different types of input data (e.g., 2D image or RGB image), the image data is input with different number of channels.

(2) Convolutional Layer

Convolutional layer is usually used to extract features and its calculation formula is as follows:

$$H_i = f(H_{i-1} \otimes W_i + b_i) \tag{10}$$

where H_t is the feature map of the i th layer, W_t is the weight vector of the i th layer, b_i is the offset vector of the i th layer, and $f(\cdot)$ is the activation function.

(3) Pooling layer

The pooling layer performs dimensionality reduction operations on the features extracted from the convolutional layer usually including the maximum pooling operation and the average pooling operation, the two pooling operations use the maximum value and the average value as the output, respectively.

(4) Fully connected layer

By linking multiple neuron structures, the fully connected layer integrates all previous features and then outputs the final complex features. Its calculation formula is as follows:

$$f(x_{in} * \omega + b) = x_{out} \tag{11}$$

In the above equation, x_{in} represents the input of the fully connected layer, x_{out} represents the output of the fully connected layer, ω represents the weight, b represents the bias, and $f(\cdot)$ represents the activation function.

(5) Output layer

The last layer of the convolutional neural network is usually used to output the final classification decision, called the output layer. Taking softmax as an example, the operation process is as follows:

$$P(C_j = j \mid x) = \frac{e^{\theta^j x}}{\sum_{j-1}^{K} e^{\theta^j x}} \tag{12}$$

In the above process, $P(C_j = j \mid x)$ represents the probability that the x th image is the j th classification, $\theta^r x$ represents the network covariates, and $\sum_{j-1}^{K} e^{\theta^r x}$ represents the normalization operation.

II. B. 2) Classical 2D Convolutional Neural Networks

Compared with other convolutional neural network structures, GoogLeNet's network structure is very complex, using multiple parallel convolutional and pooling layers, as well as multiple convolutional kernels of different sizes [19]. However, at the same time, GoogLeNet is also optimized in terms of computational and storage resources, which makes the network more efficient and practical. Moreover, GoogLeNet is the first deep convolutional neural network proposed and using Inception module. In GoogLeNet network, multiple Inception modules exist in parallel, and each Inception module extracts features from different scales through different convolutional operations, and finally splices them in the channel dimension. This operation can keep the number of computations and parameters small, avoid overfitting and improve the generalization ability of the model.

II. C. Three-dimensional convolutional neural networks

II. C. 1) Fundamentals

The output of 3D convolution is still a 3D feature map, and the convolution operation does not reduce the dimensionality of the feature map, the formula for 3D convolution is as follows:

$$V_{ij}^{pq} = \tanh(b_{ij} + \sum_{m}\sum_{p=0}^{P_i-1}\sum_{q=0}^{Q_i-1}\sum_{r=0}^{R_i-1} w_{ijm}^{pqr} v_{(i-1)m}^{(x+p)(y+q)(z+r)}) \tag{13}$$

where b_y denotes the bias and w_{ijm}^{pr} denotes the value of the convolutional kernel adjacent to the m th feature map in the previous layer at point (p,q,r).

The pooling kernel of a 3D convolutional neural network is also 3D and is formulated as follows:

$$y_{mnl} = \max_{0 \le i \le S_1, 0 \le j \le S_2, 0 \le k \le S_1}(x_{m \times s+i, n \times t+j, l \times r+k}) \tag{14}$$

where s,t,r represents the pooling step, and m,n, 1 represents the coordinates.

II. C. 2) Classical 3D Convolutional Neural Networks

S3D is a separable 3D convolutional network that reduces the number of parameters and computational complexity of the model by replacing some of the 3D convolutional layers and 3D Inception modules in the I3D network with separable convolutions.

By decomposing a 3D convolution into an ID convolution and a 2D convolution, the S3D network, based on the I3D network, retains the advantage of the I3D network in efficiently extracting temporal features while improving the efficiency of the network training, resulting in a good balance of model rate and accuracy.

II. D. Image encryption design applying 3D convolutional neural network

This time, combining CNN features and compression perception theory, by combining image encryption and compression process, first carry out the original feature extraction of the image, filter diffusion processing of the image using filters, and then combine the convolutional neural network and compression perception theory to generate the image hybrid phase mask, and finally realize the encryption protection of the image by replacing the image hybrid phase mask, the specific design is as follows [20].

II. D. 1) Extracting raw image features

Extracting the original features of an image is one of the key steps to realize image encryption.

In order to reduce the complexity of extraction when extracting the original features of the image, this time, the unit embedding distance of the data is calculated directly based on the existing data, and the similarity between these features is measured using this parameter to obtain the original features of the image. The unit embedding distance calculation formula can be expressed as:

$$L = \frac{1}{N} \times \sum(i = 1 - N)[d(i,i+1) + d(i+1,i+2)] \tag{15}$$

where N denotes the total number of pixels, $d(i,i+1)$ denotes the distance between the i th pixel point and the $i+1$ th pixel point, and $d(i+1,i+2)$ denotes the distance between the $i+1$ th pixel point and the $i+2$ th pixel point. This formula calculates the average distance between each pixel point and its neighboring pixel points as a criterion for the cell embedding distance. Assuming the Gaussian function as $G(x,y)$ and the image as I, the operation is performed to obtain the scale space, which is represented as:

$$L_1(x,y,\sigma) = \frac{G(x,y,\sigma)}{I} \times L \tag{16}$$

where (x,y,σ) denotes the operation position, I denotes the standard deviation, and $L_1(x,y,\sigma)$ denotes the scale. Based on the above, the directions are assigned, and for each point, the gradient direction of its surrounding pixels is used to assign a principal direction, which ensures rotational invariance of the descriptor. The orientation histogram is computed as:

$$H(x,y,\theta) = \sum_{i=1}^{n} m(\theta - \theta_i) \otimes L_1(x,y,\sigma) \tag{17}$$

where θ denotes the direction of the key point, θ_i denotes the gradient direction of the pixels in its neighborhood, and $\sum_{i=1}^{n} m$ denotes some kind of metric function. Using the above, the original features of the image are extracted with the formula:

$$Q = H(x, y, \theta) \cos^{-1} \rho \tag{18}$$

where ρ denotes the gradient statistical information of each cell. Through the above steps, the original features of the image are extracted.

II. D. 2) Image Filter Diffusion Processing

After the original features of the image are extracted, the image is filtered and diffused using a filter. The filter is a two-dimensional matrix whose center element is aligned with the currently processed pixel while the remaining elements correspond to the associated pixels. The output of the filter is obtained by multiplying and summing its center element with the corresponding pixel. Assuming that a second-order filter of size $a \times h$ is used in this case, the filtering function for the image is represented as follows:

$$f_Q = \sum_{i=1}^{a-1} \sum_{j=1}^{h-1} g(i, j) \times f(1+i, 1+j) \tag{19}$$

where $g(i, j)$ denotes the filter transfer function and $f(1+i, 1+j)$ denotes the corresponding pixel in the image. The formula multiplies each element of the filter by the corresponding pixel in the image and adds the results together to obtain the filtered pixel values. According to the filtering process, image filter diffusion can be performed to achieve smoothing of the image, edge detection, noise suppression, etc.

According to the diffusion schematic, when filter diffusion is performed on a pixel point, the matrix of neighboring pixels corresponding to the pixel point is T and its expression is:

$$T = \begin{bmatrix} P(l-1, l_1-1, l_3) \\ P_1(l-1, l_1, l_3) \\ P_2(l, l_1-1, l_3) \\ P_3(l, l_1, l_3) \end{bmatrix} \tag{20}$$

where $P_3(l, l_1, l_3)$ is denoted as a pixel point. The image is filtered and diffused according to the matrix of neighboring pixels corresponding to the pixel point with the expression:

$$P_3(l, l_1, l_3) = (\sum_{i=1}^{2} \sum_{j=1}^{2} T \oplus F) \bmod 256 \tag{21}$$

where mod256 denotes the modal value and F denotes the edge function, also known as the edge stopping function. In summary, the image filter diffusion processing is completed.

II. D. 3) Generating an Image Mixing Phase Mask

After completing the image filter diffusion process, the image hybrid phase mask is generated based on the convolutional neural network compression perception and its output sequence is used for the compression perception of the image. In this process, the mapping equation can be expressed as:

$$X = \mu X_T (1 - X) \tag{22}$$

where μ is denoted as the variable of the image and $1 - X$ is denoted as the output value. By updating the result with μ and $1 - X$, the phase mask CPM of the image is generated, which is expressed as:

$$R = \exp(b 2 \pi X) \tag{23}$$

where b is denoted as the number of times. According to the phase mask CPM of the image to solve the problem of CPM within the image encryption structure of the optical axis correction occurs, the SPM function formula of the image can be expressed as:

$$M(r, \beta) = \exp(d \beta R - \frac{\pi r^2}{\eta s}) \tag{24}$$

where d denotes the phase mask order, s denotes the phase mask focal length, and η denotes the light wave wavelength of the image. The polar coordinates of the image SPM in Cartesian space are described by (r, β), and the operational formula for (r, β) is:

$$\begin{cases} r = x^2 + y^2 \\ \beta = \tan^{-1}(\dfrac{1}{x} y) \end{cases} \tag{25}$$

where x denotes the horizontal coordinate data and y denotes the vertical coordinate data. Equation (24) is combined with equation (25) to obtain the hybrid phase mask of the image, which is given by:

$$W = \exp(b2\pi X) + (d\beta - \frac{\pi r^2}{\eta s})M(r,\beta) \tag{26}$$

To summarize, image hybrid phase mask is generated based on convolutional neural network compression perception algorithm.

II. D. 4)   Substitution of image mixing phase masks

After the generation of image hybrid phase mask based on convolutional neural network compression perception, it is necessary to make a finite-order element transformation of the image hybrid phase mask to disrupt the position of the pixels in the image, so as to confuse them, so that the original image can not be recognized, and to realize the encryption of the image. The initial image $PM \times N$ hybrid phase mask matrix, whose size is $M \times N$, can be shown as follows:

$$W_{M \times N} = \begin{bmatrix} W_1, W_2, ..., W_N \\ W_N, W_{N+1}, ..., W_{N(M-1)+1} \\ W_{N(M-1)+1}, W_{N(M-1)+2}, ..., W_{NM} \end{bmatrix} \tag{27}$$

where W is denoted as the hybrid phase mask. According to the hybrid phase mask matrix, setting k as the number of processors, the hybrid phase mask vector can be expressed in the following form:

$$\begin{cases} D_1 = \left[D_1, D_2, ..., D_{\frac{MN}{k}} \right] \\ D_2 = \left[D_{\frac{MN}{k}+1}, D_{\frac{2MN}{k}+1}, ..., D_{\frac{(n+1)MN}{k}} \right] \\ D_k = \left[D_{\frac{(k-1)MN}{k}+1}, D_{\frac{2(k-1)MN}{k}+1}, ..., D_{\frac{MN}{k}+1} \right] \end{cases} \tag{28}$$

where k denotes the number of processors and D denotes the hybrid phase mask vector. Based on the above results, the number of iterations is set to 200, and the resulting data can be expressed as:

$$z = mod(g_k) - floor(g_k) \times 10^4 \tag{29}$$

where (g_k) is denoted as the number of groups. Based on the above, a substitution of the image mixing phase mask can be performed to convert it to the form of a row vector. Specifically, the substitution can be performed using the following equation:

$$A = \frac{W_{M \times N}}{D_1 + D_2 + D_k} \times z \tag{30}$$

In this way, the arrangement position of the image pixels can be disturbed, and the row vector H after substitution can be used as the encrypted image data to realize the encryption of the image.

III. Prison Behavior Recognition of Prisoners Based on CNN and Image Encryption Technology

III. A. Performance Analysis of Prisoner Behavior Recognition Model for Prison Inmates

III. A. 1)   Evaluation indicators

The dataset used in this section is obtained after the construction of a convolutional neural network model and contains {number of users: 8963, number of items: 280, number of data interactions: 223421, number of entities: 9183, number of relationships: 264855, number of triples: 487963}, labeled features include suicide risk, risk of

homicide, risk of negative transformation, and there are 5 types of labels for each feature, namely No Risk, Mild Risk, Moderate Risk, High Risk, Extremely High Risk, and each labeled feature is mapped to 5 corresponding item entities in the knowledge graph, benchmarking the click-through rate prediction task in the recommender system. The ratio of risk to no risk in the assault data and suicide data is about 3:5, the label of the former is the risk level assessed by the supervisors based on the number of real assaults in the history of the offender in the prison punishment information table, the label of the latter and the label of the passive rehabilitation is the risk level assessed by the supervisors based on the offender's historical performance combined with their own work experience, and the ratio of risk to no risk in the passive rehabilitation data is about 1:10.

In this experiment, AUC, accuracy, recall, and $F1$ are used as evaluation metrics. With TP as the true case, FP as the false positive case, FN as the false negative case, and TN as the true negative case, the formula of accuracy rate is shown in (31):

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{31}$$

The formula for recall is shown in (32):

$$Recall = \frac{TP}{TP+FN} \tag{32}$$

The formula for $F1$ is shown in (33):

$$F1 = \frac{2 \times TP}{2 \times TP+FN+FP} \tag{33}$$

III. A. 2) Performance analysis

Taking the accuracy rate as the evaluation index, the prediction effect of the three abnormal behaviors is verified separately, and the experimental comparison results of the proposed model with other algorithms are shown in Fig. 3.

The accuracy rate of the abnormal risk assessment for each model for performing murder is better than the suicide and negative transformation assessment accuracy rate. Taking the method of this paper as an example, the percentage of accuracy rate of the risk assessment of performing murder is 94.1358%, which is higher than 91.0988% and 91.1554% of suicide and negative rehabilitation. The analysis shows that the proportion of no risk in the assault risk data is larger, and because the label of assault risk is assessed by the supervisors based on the recent history of real assault performance, the label of the state information of the sentenced person is more accurate: while there are more risk labels in the data distribution of the suicide risk and the negative rehabilitation risk and the labels are assessed by the supervisors based on the human experience, and they are highly subjective. In each case, the method of this paper is better than other models, which proves the superiority of the method.
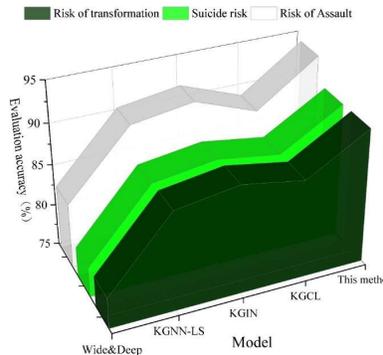

Figure 3: Abnormal risk assessment of different model prediction performance

In order to verify the effect of the number of graph convolutional network layers on the experimental performance, the overall prediction results of the three abnormal behaviors were designed to be tested by the model when the graph convolutional layer L was 1,2,3,4, respectively, and the experimental comparison results are shown in Fig. 4.

When the number of graph convolution layers is 2, the model reaches the optimal performance, at this time, the AUC, accuracy, recall, and F1 value are 96.2645%, 92.1685%, 88.2498%, and 85.7174%, respectively, and with the deepening of the network structure, the model will be overfitting phenomenon, and the experimental effect decreases. According to the above experiments, the effectiveness and superiority of the method proposed in this paper are fully proved in the task of abnormal risk assessment of specific populations.
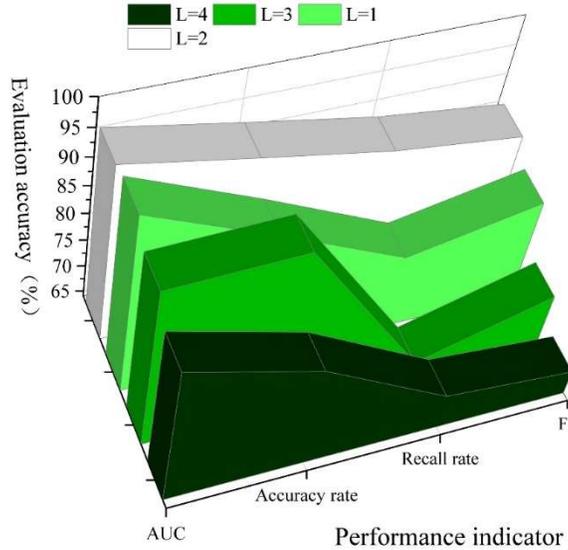

Figure 4: The predictive energy of the abnormal risk assessment of different volumes

III. B. *Prison Behavior Dataset for Prisoners*

Currently, most of the publicly available datasets are intercepted fragments from some websites with complex and useless backgrounds, which greatly increases the cost of behavior recognition. In order to verify the effectiveness of the proposed model in real-life scenarios, a dataset of daily and abnormal behaviors of prison inmates is collected.

In order to verify that the convolutional neural network can be applied in real life scenarios, in this subsection, we simulate the corridor scene of the inmates in prison and use the video surveillance angle to collect a small video dataset, the location of the collection is a straight corridor, in the corridor there are two different angles of the surveillance camera, the captured person in the monitoring camera's visual range of the corresponding behavior.

The prison behavior dataset of the inmates mainly includes three kinds of abnormal behaviors: fighting, attacking the police, and falling down, and two kinds of daily behaviors: carrying and handing things. The total duration of the dataset is about 2 hours, with 710 video samples, and the average duration of the samples is about 10 seconds. The information related to the amount of data for each action in the prison behavior dataset of prison inmates is shown in Table 1, and the prison inmates' daily behaviors account for the largest proportion of moving things, with 200 pieces of data, accounting for 28.169%.

Table 1: The prison data set each action sample volume related information

Serial number	Behavior type	Data volume	Quantity ratio
1	Fight	156	21.9718%
2	Attack	140	19.7183%
3	Fall	138	19.4366%
4	Carry	200	28.1690%
5	Pass	76	10.7042%
Total	-	710	100.0000%

IV. Research on behavioral monitoring of prison inmates

IV. A. Behavioral Monitoring Analysis Results

IV. A. 1) Abnormal Behavior Scores of Sentenced Persons Based on Time Distribution

The sensitivity scores of prison inmates are arranged in a time series in order to conduct a study on the changes in the psychological state of prison inmates. Among many research subjects, this paper selects two serving prisoners with certain representativeness as examples.Figure 5 shows the abnormal behavior scores of serving prisoners based on the time distribution, Figure (a) is No. 735, and Figure (b) is No. 1058.No. 735 shows a relatively calm performance in early June, but there is a clear peak of abnormal behavior at the end of the month (24th), with an abnormality score of 306,745 points.1058 No. 1058's sensitivity score in June showed a clear high-risk trend, and on June 24th it was 675,085, close to 700,000, which is a typical change in behavioral status that is gradually deepened by the influence of factors in the sensitive area, and it can basically be judged that his correctional situation has deteriorated, and he needs to be intervened in a timely manner by supervisory and counseling staff.
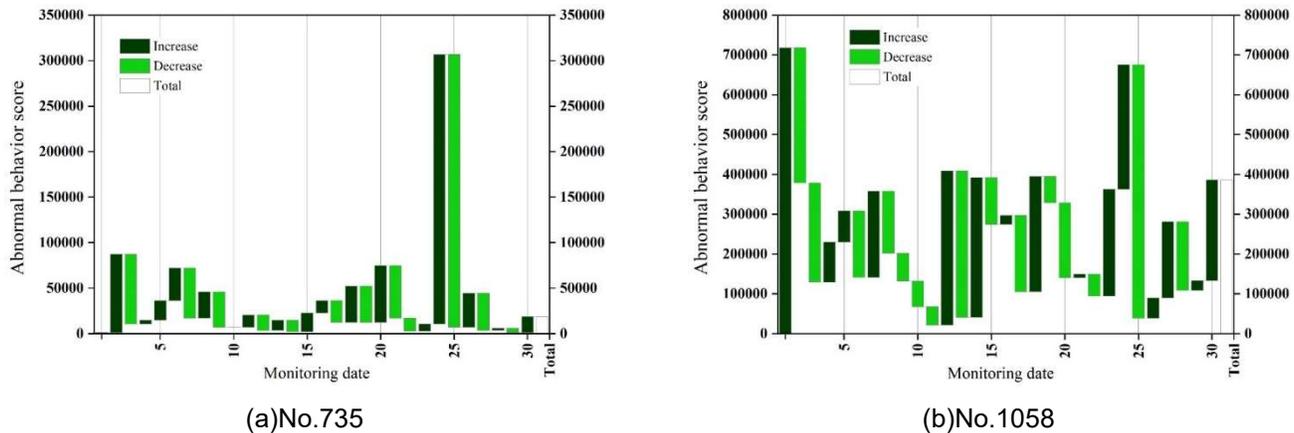

(a)No.735　　　　　　　　　　　(b)No.1058

Figure 5: A time distribution of a prison man's abnormal behavior score

IV. A. 2) Effectiveness of manual intervention on abnormal behavior

The statistical results of the weekly scores of the five selected inmates in May-June are shown in Fig. 6, in which the scores of No. 2682, 2593 and 2515 are higher, and the mean values of the 8-week data are 2137832, 469457 and 232430, respectively, and the scores of No. 1836 and 1375 are lower. After the managers analyzed the abnormal behavior scores in May 2023, they intervened to stop and criticize and educate the higher scores of No. 2682 and No. 2515, so the abnormal behavior conditions of the two inmates were significantly alleviated in June, and basically restored to the normal activity status with lower scores. On the other hand, No. 2593, who was not intervened, still had a higher wave of sensitive scores in June, and was in the same state as the sensitivity level in May.
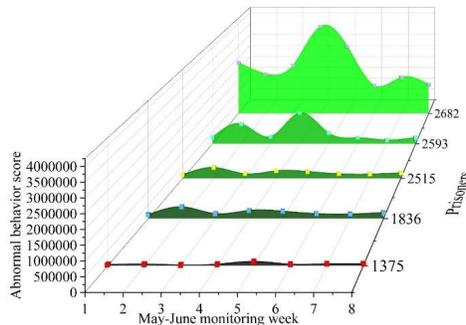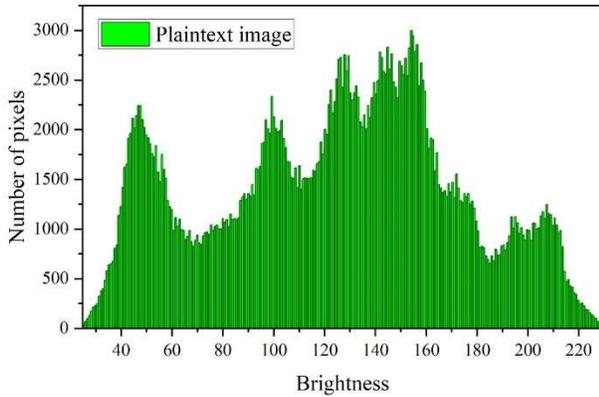

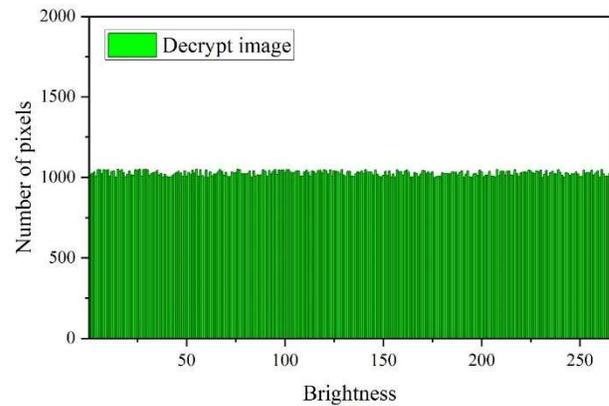Figure 6: Comparison of artificial intervention abnormal behavior scores

IV. B. Image encryption results

Image histograms can be used to represent the statistical characteristics of image data. In the image histogram, the horizontal coordinate is the pixel value and the vertical coordinate is the number of times a pixel value appears in the whole image. Fig. 7 shows the image processing histogram based on convolutional neural network image
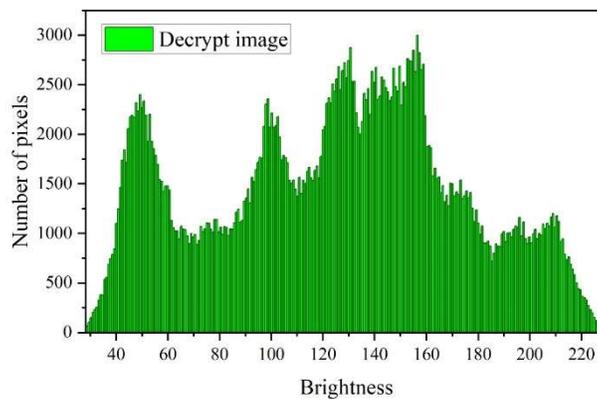
encryption technique, Figs. (a)-(c) show the histograms of plaintext image, ciphertext image and decrypted image respectively. The pixel values of the encrypted image in Fig. (b) are nearly uniformly distributed over the interval [0,255], and the number of occurrences of the pixel values ranges from 1000 to 1050 times, which can hide the statistical features of the plaintext image well. As can be seen from Fig. (c), the decrypted image completely retains the information of the plaintext image. Therefore, the algorithm can effectively encrypt the behavioral images of prison service personnel.

(a)The histogram of the plaintext image

(b)The histogram of the ciphertext image

(c)Decrypt the histogram of the image

Figure 7: Histograms of plaintext images and ciphertext images

V. Conclusion

Convolutional neural network image encryption technology shows superior performance in monitoring the behavior of prison inmates. The results of the model evaluation show that the accuracy of the identification of homicide risk reaches 94.14%, which is significantly higher than the identification of suicide risk 91.10% and the identification of negative rehabilitation risk 91.16%. This result reflects that the model is more effective in recognizing risk types with clear historical performance indicators. The overall performance of the model is optimal when the number of graph convolution layers is 2, achieving an AUC value of 96.26%, an accuracy rate of 92.17%, a recall rate of 88.25%, and an F1 value of 85.72%. More than 2 layers leads to overfitting phenomenon and a decreasing trend in performance.

The time series analysis reveals that the abnormal behavior of the prison inmates shows obvious volatility. For example, No. 1058 sentenced personnel's abnormal score was as high as 675085 points on June 24, showing a trend of deepening influence by sensitive regional factors. The analysis of the effect of manual intervention shows that the intervention of stopping and criticizing the education of inmates No. 2682 and No. 2515 has significantly alleviated their abnormal behavioral conditions and restored them to the normal activity state in the following month;

in contrast, No. 2593, which has not been intervened, still maintains a high sensitivity score state in the following month.

For image encryption processing, the pixel values of the encrypted image are nearly uniformly distributed in the 0-255 interval, and the number of occurrences of the pixel values is kept between 1000-1050 times, which effectively hides the statistical features of the plaintext image, while the decrypted image completely retains the original information. This technology provides data security for the behavioral monitoring of prison inmates, and combined with the behavioral recognition capability of convolutional neural network, it constitutes a complete intelligent management solution for prisons, which has practical application value for promoting the modernized management of prisons.

References

[1]   Knight, V., & Van De Steene, S. (2017). The capacity and capability of digital innovation in prisons: Towards smart prisons. Advancing Corrections, 4(8), 88-101.

[2]   Ganbadrakh, T. A. (2017). The Impact of Information and Communication Technologies on Prison Institutions. Military Engineer/Hadmérnök, 12(1).

[3]   Pan, T. (2022). Intelligent Monitoring System for Prison Perimeter Based on Cloud Intelligence Technology. Wireless Communications and Mobile Computing, 2022(1), 2517446.

[4]   Belur, J., Thornton, A., Tompson, L., Manning, M., Sidebottom, A., & Bowers, K. (2020). A systematic review of the effectiveness of the electronic monitoring of offenders. Journal of Criminal Justice, 68, 101686.

[5]   Law, P. C., Wang, Y. L., Poon, L. C., Chung, A. W., & Lai, K. W. (2020, October). Smart prison-video analysis for human action detection. In IECON 2020 the 46th Annual Conference of the IEEE Industrial Electronics Society (pp. 513-516). IEEE.

[6]   Mabrouk, A. B., & Zagrouba, E. (2018). Abnormal behavior recognition for intelligent video surveillance systems: A review. Expert Systems with Applications, 91, 480-491.

[7]   Bouachir, W., Gouiaa, R., Li, B., & Noumeir, R. (2018). Intelligent video surveillance for real-time detection of suicide attempts. Pattern Recognition Letters, 110, 1-7.

[8]   Michaud, L., & van der Meulen, E. (2023). "They're Just Watching You All the Time": the surveillance web of prison needle exchange. Surveillance & society, 21(2), 154-170.

[9]   Kaun, A., & Stiernstedt, F. (2020). Doing time, the smart way? Temporalities of the smart prison. New Media & Society, 22(9), 1580-1599.

[10] Aktı, Ş., Tataroğlu, G. A., & Ekenel, H. K. (2019, November). Vision-based fight detection from surveillance cameras. In 2019 Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA) (pp. 1-6). IEEE.

[11] Andrejevic, M. (2019). Automating surveillance. Surveillance & society, 17(1/2), 7-13.

[12] Fedorczyk, F. (2024). Navigating the dichotomy of smart prisons: between surveillance and rehabilitation. Law, Innovation and Technology, 16(1), 243-260.

[13] Sabri, Z. S., & Li, Z. (2021). Low-cost intelligent surveillance system based on fast CNN. PeerJ Computer Science, 7, e402.

[14] Onyema, E. M., Balasubaramanian, S., Iwendi, C., Prasad, B. S., & Edeh, C. D. (2023). Remote monitoring system using slow-fast deep convolution neural network model for identifying anti-social activities in surveillance applications. Measurement: Sensors, 27, 100718.

[15] Ramachandran, S., & Palivela, L. H. (2019). An intelligent system to detect human suspicious activity using deep neural networks. Journal of Intelligent & Fuzzy Systems, 36(5), 4507-4518.

[16] Vosta, S., & Yow, K. C. (2022). A cnn-rnn combined structure for real-world violence detection in surveillance cameras. Applied Sciences, 12(3), 1021.

[17] Saeed Omidi & Yevgeny Berdichevsky. (2025). Pathway-like Activation of 3D Neuronal Constructs with an Optical Interface. Biosensors,15(3),179-179.

[18] Oliver W. Layton,Siyuan Peng & Scott T. Steinmetz. (2024). ReLU, Sparseness, and the Encoding of Optic Flow in Neural Networks. Sensors,24(23),7453-7453.

[19] G. Sekar,Benson Mansingh,Joghee Prasad & R. Nallakumar. (2025). Convolutional Neural Network Based Quality Analysis of Fruits and Vegetables. Applied Mechanics and Materials,926,151-162.

[20] Jingang Liu,Guorui Cheng & Shenmin Song. (2025). Event-triggered distributed diffusion robust nonlinear filter for sensor networks. Signal Processing,226,109662-109662.