Hindawi
Complexity
Volume 2018, Article ID 8524825, 12 pages
https://doi.org/10.1155/2018/8524825

Research Article

Research on Face Recognition Method by Autoassociative Memory Based on RNNs

Qi Han,[1,2] Zhengyang Wu,[3] Shiqin Deng,[1] Ziqiang Qiao,[4] Junjian Huang,[2] Junjie Zhou,[5] and Jin Liu[3]

[1] *Intelligent School of Technology and Engineering, Chongqing University of Science and Technology, 401331 Chongqing, China*
[2] *Key Laboratory of Machine Perception and Children's Intelligence Development, Chongqing University of Education, 400067 Chongqing, China*
[3] *College of Safety Engineering, Chongqing University of Science and Technology, 401331 Chongqing, China*
[4] *China United Engineering Corporation Limited, 310052 Hangzhou, Zhejiang, China*
[5] *Chongqing Energy Investment Group Science and Technology Co., Ltd., 400061 Chongqing, China*

Correspondence should be addressed to Jin Liu; Liujin@cqust.edu.cn

Received 11 May 2018; Revised 28 September 2018; Accepted 8 October 2018; Published 2 December 2018

Academic Editor: Chongyang Liu

In order to avoid the risk of the biological database being attacked and tampered by hackers, an Autoassociative Memory (AAM) model is proposed in this paper. The model is based on the recurrent neural networks (RNNs) for face recognition, under the condition that the face database is replaced by its model parameters. The stability of the model is proved and analyzed to slack the constraints of AAM model parameters. Besides, a design procedure about solving AAM model parameters is given, and the face recognition method by AAM model is established, which includes image preprocessing, AAM model training, and image recognition. Finally, simulation results on two experiments show the feasibility and performance of the proposed face recognition method.

1. Introduction

With the development of information and Internet, biometric technology has been rapidly developed for security, confidentiality, and convenience in Internet applications. Nowadays, many biometric technologies have been developed, such as fingerprint recognition, face recognition, and iris recognition [1, 2]. Among them, face recognition is one of the most widely used biometric technologies [3]. However, these technologies may be still vulnerable to sophisticated hacker attacks. N. Ratha et al. [4, 5] summed up eight basic threats that plague biometric-based authentication systems. One of vulnerabilities (Threat 6) is that it is possible to modify templates in the biological database or insert templates from unauthorized users into the biological database [6]. Biometric templates are a set of stored biometric features comparable directly to probe biometric features [7].

In recent years, substantial research has been conducted to improve operation security in view of the above threats, especially the protection of biometric template database for Threat 6. Biometric template protection schemes have been divided into Cancelable Biometrics (CBs), Biometrics Cryptosystems (BCs) and Biometrics in the Encrypted Domain (BED) [8]. CBs are to use noninvertible transformation to convert the original biometric data into intentionally distorted information [9]. In [10], it proposed a new method for the design of alignment free cancelable fingerprint templates using local minutia structures formed by zoned minutia pairs. A novel cancelable biometric template generation algorithm using Gaussian random vectors and one way modulus hashing was proposed in [11]. In BCs, a key is either bound (key binding schemes) or extracted (key generation schemes) from biometric data [8]. The key binding schemes can be classified as fuzzy vault schemes [12] and the fuzzy commitment schemes [13]. Regarding key generation schemes, a number of discretized fingerprint descriptors and appropriate error correcting codes were used to propose an effective biometric cryptosystem construction for biometric template protection in [14]. However, as in the case of CBs, CBs usually present a performance degradation with respect to the systems relying on unprotected data [8]. From this secure multiparty computation and homomorphic cryptosystems were used to carry out BED [15]. At present, current approaches to BED are based on garbled circuits [16] and homomorphic encryption [15], but these schemes are much more complex than the representations used in the aforementioned articles [17].

Although these schemes achieved some success, they do not completely eliminating the risk of hacker attacking and tampering the templates. There is no doubt that the existence of the template database is a hidden danger to public security [8]. In order to tackle this problem, a new face recognition method by associative memory (AM) is proposed in this paper. Although we focus on face recognition throughout this paper, our study can be extended to other biometric authentication methods.

Associative memories (AMs) are brain-style devices designed to store a set of patterns as stable equilibria such that the stored patterns can be reliably retrieved with the initial probes containing sufficient information about the patterns [18]. AMs can be divided into Autoassociative Memory (AAM) and Hetero-Associative Memory (HAM) [18]. When the input I and the output α are identical, α is said to be memorized with I in the AAM, whereas α is said to be memorized with I in the HAM. In recent years, AMs, especially the AMs based recurrent neural networks (RNNs), have been widely studied. For example, in [19], a synthesis procedure for designing associative memories based on discrete-time recurrent neural networks (DTRNNs) was presented and the global convergence of the DTRNNs was guaranteed via the stability analysis. In order to get some broad conditions for design cloning templates of RNNs, some new methods about associative memories based on RNNs with time delay are given in [20]. Meanwhile, in the research process of AM based on RNNs, the stability of RNNs plays a decisive role in the realization of associative memory. In [21–23], the stability of RNNs is studied systematically. Besides, the RNNs were also widely used in many fields [24, 25]. However, if we want to better realize associative memory among facial features, the constraints of the current AM based RNNs are still relatively conservative. Therefore, it is necessary to use stability analysis to slack the constraints and apply them to face recognition.

Based on the aforementioned discussion, the main contributions of this paper are listed as follows:

(1) To protect the face features database fundamentally, a new face recognition method by AAM based on RNNs is proposed without establishing face feature database, in which the face features are transformed into the parameters of the AAM model.

(2) An AAM model based on RNNs with a tunable slope activation function is proposed, which is different from the work of [20, 21] that only discusses on Autoassociative Memory at the fixed slope activation function.

(3) The constraints of AAM model parameters are relaxed by our theories. It provides a theoretical basis for ensuring the effectiveness of face recognition.

The rest of this paper is organized as follows. The overview of the proposed method is elaborated in Section 2. In Section 3, we propose an AAM model based on RNNs, then the stability of the model is analyzed in detail, and its design procedure is given. In Section 4, a face AAM recognition method is established. Two experiments are presented in Section 5. Finally, conclusions are drawn in Section 6.

2. Overview of the Method

In order to solve a problem of hacker attacking and tampering the templates, a face recognition method by AAM based on RNNs is proposed in absence of the biometric database, as shown in Figure 1.

The common method of face recognition is usually to compare the facial features collected on site with those in the face database one by one, and then to determine whether if it has access right based on their similarity. In contrast, the method proposed in this paper is not to establish a face database, but to set up some special kind of relationship between facial features of authorized users. This relationship is stored in the model parameters after AAM training. Therefore, the relationship is unique because model parameters will vary with the authorized users.

For example, there are four users, respectively are A, B, C, and D. If the users A, B, and C have access right, and the user D has no access right, the model parameters Pm_1 can be obtained by AAM training of the facial features of users A, B, and C, where the user C can achieve AAM, while the user D cannot. Similarly, if the users A, B, and D have access right, and the user C has no access right, the model parameters Pm_2 can be obtained by associative memory training of the facial features of users A, B, and D, where the user D can achieve AAM, while the user C cannot. Obviously, the model parameters Pm_1 and Pm_2 are completely different due to due to the uniqueness of each user's facial features. Therefore, it could realize face recognition without establishing the face database, where facial features of authorized users are converted to model parameters. The specific face recognition method is as follows.

At the registration stage, under the condition that the face features of the authorized users are extracted, AAM model parameters are obtained by AAM training where its input and output are coming from facial features from the extracted authorized users. Therefore, the special relationship between authorized users' facial features has been stored in the AAM model parameters due to the uniqueness of each user's facial features.

At the recognition stage, when a user accesses the face recognition system, the user's facial features are first obtained through a feature extractor and then are entered into the trained AAM model to get its output features. Whether the visitor can access is determined by its similarity between the input features and the output features.

In the face identification, authorized users can successfully pass identification detection because of the special relationship (AAM model parameters), whereas unauthorized users cannot.

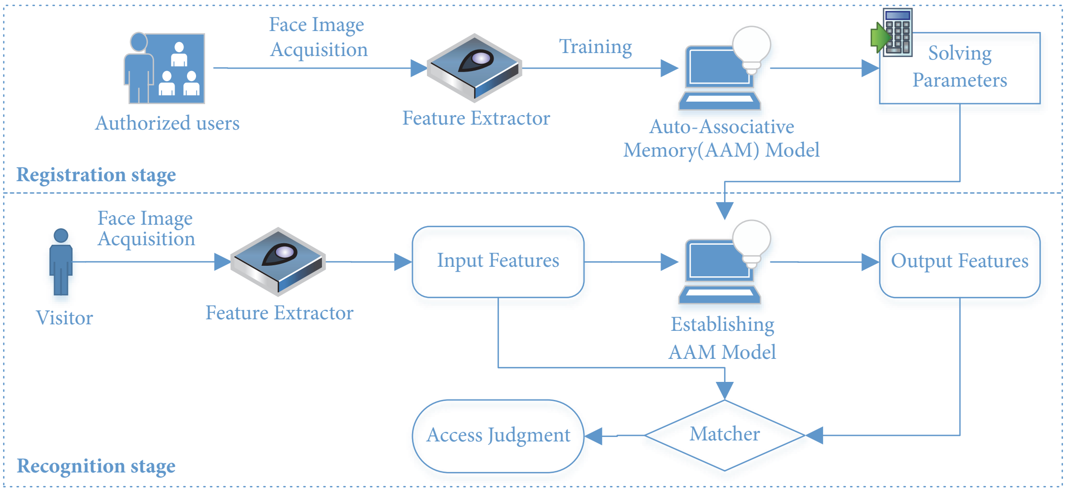


Figure 1: Flowcharts of the face recognition method by AAM based on RNNs.

3. Technical Solutions

The face recognition method proposed in this paper is implement through AAM based on RNNs. Therefore, this section first proposes an AAM model based on RNNs for face recognition system, where a tunable slope activation function is given. Meanwhile, in order to slack the constraint conditions of the model, its stability is proved and analyzed by 2 Theorems and 2 corollaries. Finally, in order to guarantee the implementation of the associative memory function of face recognition method, the associative memory process of AAM model based on RNNs is discussed and its design procedure is given.

3.1. An AAM Model. In this subsection, an AAM model based on RNNs is proposed as follows:

$$\dot{\xi}(t) = -A\xi(t) + Bf(\xi(t)) + CI + D \tag{1}$$

$$y(t) = f(\xi(t)) \tag{2}$$

where $\xi(t) = (\xi_1(t), \xi_2(t), \ldots, \xi_n(t))^T \in R^n$ denotes a neuron state vector, $A = \mathrm{diag}[a_1, a_2, \ldots, a_n]$ is a constant diagonal matrix forming the self-regulating parameter of the neuron, $B = (b_{ij})_{n\times n}$ and $C = (c_{ij})_{n\times n}$ are the connection weight matrixes, $D = (d_1, d_2, \ldots, d_n)^T_{n\times 1}$ is an offset vector, $I = (I_1, I_2, \ldots, I_n)^T_{n\times 1}$ stands for an input pattern and $f(\xi_i) = \lambda/2h \cdot (|\xi_i + h| - |\xi_i - h|)$ denotes a tunable slope activation function, in which $\lambda\,(\lambda > 0)$ is a parameter associated with memory patterns, and $h\,(h > 0)$ is a tunable parameter for better memory performances and making convergence fast. It is obvious that once ξ_i fall into $(-\infty, -h)$ or $(h, +\infty)$, the tunable slope activation function's value will no longer change, and this means that the output of the neural network becomes stable.

Remark 1. The definitions of the connection weight matrixes B and C are given in Appendix A.

Let

$$\begin{aligned} \alpha \in \varphi = {} & \left\{y = (y_1, y_2, \ldots, y_i, \ldots, y_n)^T \in R^n \mid y_i = \lambda \text{ or } \right. \\ & \left. -\lambda,\ i = 1, 2, \ldots, n\right\} \\ \vartheta(\alpha) = {} & \left\{z = (z_1, z_2, \ldots, z_i, \ldots, z_n)^T \in R^n \mid z_i\alpha_i > h,\ i \right. \\ & \left. = 1, 2, \ldots, n\right\} \end{aligned} \tag{3}$$

According to the lemma of [26], for all i in (1), we have $f(\xi) = \alpha\,(|\xi_i| \geq h)$, when tunable slope activation function converges to a stable state. For all $\xi \in \vartheta(\alpha)$, (1) can be rewritten as

$$\dot{\xi}(t) = -Ax(t) + B\alpha + CI + D \tag{4}$$

Equation (4) can be transformed as

$$\dot{\xi}_i(t) = -a_i\xi_i(t) + b_{ii}\alpha_i + w_i, \quad i = (1, 2, \ldots, n) \tag{5}$$

where

$$w_i = \sum_{j=1, i\neq j}^{n} b_{ij}\alpha_j + \sum_{j=1}^{n} c_{ij}I_j + d_i \tag{6}$$

Moreover, we define $\delta_{ii} = 1/b_{ii}$, $b_{ii} \neq 0$, and $\delta_{ii}a_i$ is the slope factor.

3.2. Stability Analysis. On the basis of the new tunable slope activation function mentioned above, it is necessary for the AAM model to attain stability under different slope factors. The stability constraints that the model needs to satisfy are given through the following theorems and corollaries.

Theorem 2. *In (5), choose* $0 < \delta_{ii}a_i \leq 1/h$.

(I) When $w_i > \lambda/\delta_{ii} - a_i h$, *(5) converges to a stable state, and its value is bigger than* h.

(II) When $w_i < a_i h - \lambda/\delta_{ii}$, *(5) converges to a stable state, and its value is smaller than* $-h$.

Remark 3. The proof of Theorem 2 is in Appendix B.

Theorem 4. *In (5), let $-\infty < \delta_{ii}a_i < 0$ or $1/h < \delta_{ii}a_i < +\infty$.*

(I) When $w_i \geq a_i h - \lambda/\delta_{ii}$, (5) converges to a stable state, and its value is bigger than h.

(II) When $w_i \leq \lambda/\delta_{ii} - a_i h$, (5) converges to a stable state, and its value is smaller than $-h$.

Remark 5. The proof of Theorem 4 is similar to that of Theorem 2.

On the basis of the above theorems, if we choose $\eta > 1$, we can draw the following corollaries.

Corollary 6. *From Theorem 2, let $0 < \delta_{ii}a_i \leq \lambda/h$.*

(I) When $w_i = \eta(\lambda/\delta_{ii} - a_i h)$, (5) converges to a stable state, and its value is bigger than h.

(II) When $w_i = \eta(a_i h - \lambda/\delta_{ii})$, (5) converges to a stable state, and its value is smaller than $-h$.

Corollary 7. *From Theorem 4, let $-\infty < \delta_{ii}a_i < 0$ or $\lambda/h < \delta_{ii}a_i < +\infty$.*

(I) When $w_i = \eta(a_i h - \lambda/\delta_{ii})$, (5) converges to a stable state, and its value is bigger than h.

(II) When $w_i = \eta(\lambda/\delta_{ii} - a_i h)$, (5) converges to a stable state, and its value is smaller than $-h$.

Remark 8. From the above two corollaries, one can draw a conclusion that the constraints, parameters of the model in [19, 20] needing to meet, are conservative compared with the constraints proposed in this paper. In other words, the constraints of the model parameters proposed in this paper are relatively slack.

3.3. Associative Memory. Next, we will discuss associative memory process of AAM model based on RNNs by use of the above theories.

In the subsection, the explanation of new notation can be found in Appendix C. Under different conditions, the associative memory parameters' acquisition process of AAM model is as follows:

(I) According to Corollary 6 and (5), when $0 < \delta_{ll}a_l \leq \lambda/h$, $l \in \{1, 2, \ldots, n\}$, we can conclude that

$$\left(B - B'\right)\Gamma + CI' + D' = \eta\left(\frac{\lambda}{\delta_{ll}} - a_l h\right)\Upsilon, \tag{7}$$

where $\eta > 1$.

Equation (7) can be transformed as

$$\Theta^{(l)} {L_b}^{(l)} + \mathrm{T}^{(l)} {L_c}^{(l)} + D^{(l)} = \eta\left(\frac{\lambda}{\delta_{ll}} - a_l h\right)\hat{\Upsilon}^{(l)} \tag{8}$$

$$\Downarrow$$

$$\begin{aligned}&\left(\Theta^{(l)}, \mathrm{T}^{(l)}, e\right)\left(\left({L_b}^{(l)}\right)^T, \left({L_c}^{(l)}\right)^T, D^{(l)}\right)\\ &\quad = \left(\Theta^{(l)}, \mathrm{T}^{(l)}, e\right) L_{con}^{(l)} = \eta\left(\frac{\lambda}{\delta_{ll}} - a_l h\right)\hat{\Upsilon}^{(l)}\end{aligned} \tag{9}$$

Theorem 9. *In (9), $L_{con}^{(l)} = pinv(\Theta^{(l)}, \mathrm{T}^{(l)}, e)\eta(\lambda/\delta_{ll} - a_l h)\hat{\Upsilon}^{(l)}$, $(\lambda > 0, l \in \{1, 2, \ldots, n\})$ is a least square solution of (9).*

Remark 10. The proof of Theorem 9 is in Appendix D.

Obviously, when $0 < \delta_{ll}a_l \leq \lambda/h$, $l \in \{1, 2, \cdots, n\}$, the corresponding parameters of the AAM model can be obtained by Theorem 9.

(II) According to Corollary 7 and (5), when $-\infty < \delta_{ll}a_l < 0$ or $\lambda/h < \delta_{ll}a_l < +\infty$, $l \in \{1, 2, \ldots, n\}$, we can conclude that

$$\left(B - B'\right)\Gamma + CI' + D' = \eta\left(a_l h - \frac{\lambda}{\delta_{ll}}\right)\Upsilon \tag{10}$$

where $\eta \geq 1$.

Equation (10) can be transformed as

$$\Theta^{(l)} {L_b}^{(l)} + \mathrm{T}^{(l)} {L_c}^{(l)} + D^{(l)} = \eta\left(a_l h - \frac{\lambda}{\delta_{ll}}\right)\hat{\Upsilon}^{(l)} \tag{11}$$

$$\Downarrow$$

$$\begin{aligned}&\left(\Theta^{(l)}, \mathrm{T}^{(l)}, e\right)\left(\left({L_b}^{(l)}\right)^T, \left({L_c}^{(l)}\right)^T, D^{(l)}\right)\\ &\quad = \left(\Theta^{(l)}, \mathrm{T}^{(l)}, e\right) L_{con}^{(l)} = \eta\left(a_l h - \frac{\lambda}{\delta_{ll}}\right)\hat{\Upsilon}^{(l)}\end{aligned} \tag{12}$$

Theorem 11. *In (12), $L_{con}^{(l)} = pinv(\Theta^{(l)}, \mathrm{T}^{(l)}, e)\eta(a_l h - \lambda/\delta_{ll})\hat{\Upsilon}^{(l)}$, and $(\lambda > 0,\ l \in \{1, 2, \ldots, n\})$ is a least square solution of (12).*

Remark 12. The proof of Theorem 11 is similar to that of Theorem 9.

Obviously, when $-\infty < \delta_{ll}a_l < 0$ or $\lambda/h < \delta_{ll}a_l < +\infty$, $l \in \{1, 2, \ldots, n\}$, the corresponding parameters of the AAM model can be obtained by Theorem 11.

The parameters of the AAM model can be obtained by the aforementioned associative memory parameters' acquisition process. Therefore, under the known associative memory parameters, the associative memory process is described as follows.

According to [19], denote $\{-1, 1\}^{n_1} \times \{-1, 1\}^{n_2}$ as the product of the set of n_1-dimensional and n_2-dimensional bipolar vectors, where $\{-1, 1\}^{n_*} = \{\xi \in R^n, \xi = (\xi_1, \xi_2, \ldots, \xi_{n_*})^T, \xi_i = 1 \text{ or } -1, i = 1, 2, \ldots, n_*\}$, and $n_* = n_1$ or n_1. Given ψ ($\psi \leq \min\{2^{n_1}, 2^{n_2}\}$) pairwise vectors (memory patterns and input patterns), $(\alpha_1, I_1), (\alpha_2, I_2), \ldots, (\alpha_m, I_m) \in \{-1, 1\}^{n_1} \times \{-1, 1\}^{n_2}, m \in \{1, 2, \ldots, \psi\}$, design an AAM based on a RNN such that if I_k ($k \in \{1, 2, \ldots, m\}$) is fed to the AM from its input, then the output vector of RNNs converges to corresponding pattern α_k, $k \in (1, 2, \ldots, m)$, where $\alpha_k = I_k$.

Next, we give the design procedure of AAM based on RNNs by use of above the associative memory parameters' acquisition process and associative memory process. See Procedure 1.

Synthesize the AAM model with the connection weight matrixes A, B, and C and bias vector D. From the above procedure, an AAM model can be obtained.

```
for $i$=1 to $m$, $m \in \{1, 2, \ldots, \psi\}$
    $I_i$=input pattern (which can be a picture); %$I_i$ is a vector with $n$ rows
    $\alpha_i$=output pattern (which can be a picture); %$\alpha_i$ is a vector with $n$ rows
end for
for $l$=1 to $n$
    $a_l$=constant; $b_{ll}$=constant;
end for
Get coefficient matrix $A$ from $a_l$;
$h$=constant; $\lambda$=constant;
Get matrix $\Theta$ and $\Upsilon$ from memory patterns; get matrix $T$ from input patterns;
Get matrices $\Theta^{(l)}, T^{(l)}$ and vector $\widehat{\Upsilon}^{(l)}$ from $\Theta$, $\Upsilon$ and $T$;
for $l$=1 to $n$
    $\widehat{R}_{ll} a_l = \frac{a_l}{b_l}$;
end for
$e$=1;
for $l$=1 to $n$
    If $0 < \delta_{ll} a_l \leq \lambda/h$
        let $\eta$ =constant > 1 and $L_{con}^{(1)} = pinv(\lambda\Theta^{(l)}, T^{(l)}, e)\eta(\lambda/\delta_{ll} - a_l h)\widehat{\Upsilon}^{(l)}$;
    else
        let $\eta$ =constant > 1 and $L_{con}^{(1)} = pinv(2\Theta^{(l)}/h, \widehat{T}^{(l)}, e^T)\eta(a_l h - \lambda/\delta_{ll})\widehat{\Upsilon}^{(l)}$;
    end if
    Get ${L_b}^{(l)}, {L_c}^{(l)}, D^{(l)}$ from $L_{con}^{(l)}$;
end for
Get coefficient matrix $B$, $C$, and bias vector $D$ by use of ${L_b}^{(l)}, {L_c}^{(l)}, D^{(l)}$ from $L_{con}^{(l)}$;
```

Procedure 1

4. The Face Recognition Method

In this section, according to the stability analysis and the procedure of AAM model based on RNNs in Section 3, the face recognition method by AAM model is established. As shown in Figure 2, the method can be divided into three parts, namely, image preprocessing, model training, and face image recognition.

Step 1 (image preprocessing). Firstly, in the ORL database, selecting $m = m' \times \partial$ face images deriving from m' different people where ∂ face images are chosen for every authorized user. All the face images obtained in the ORL database are converted to the grayscale matrixes which have $n = N \times M$ elements. Then, by setting the gray threshold $\zeta = 120$, the m grayscale matrixes are further transformed into binary input matrixes $I_1, I_2, \ldots, I_m$ and binary output matrixes $\alpha_1, \alpha_2, \ldots, \alpha_m$, respectively, where $I_i = \alpha_i$, $i \in (1, 2, \ldots, m)$.

Remark 13. The element values in binary input/output matrixes are λ or $-\lambda$.

Step 2 (AAM model training). $(I_1, \alpha_1), (I_2, \alpha_2), \ldots, (I_m, \alpha_m)$ are regarded as pairwise matrixes. Obviously, (I_i, α_i) $i \in (1, 2, \ldots, m)$ represents an input-output mode group. The m input matrixes $I_1, I_2, \ldots, I_m$ are input into the AAM model based on RNNs, then the AM model is trained by the AAM procedure designed in Section 3.3. Finally, the AAM model parameters ${L_b}^{(l)}, {L_c}^{(l)}, D^{(l)}$, $l \in (1, 2, \ldots, n)$ are derived from AAM training. Thus, the AAM model based on RNNs is established.

Step 3 (image recognition). During the recognition process, if someone wants to access a face recognition system, the person's face image will be obtained. By image preprocessing method in Step 1, the corresponding binary input matrix I can be obtained. If binary input matrix I is input into the established AAM model, the corresponding binary output matrix α will be gotten by AAM. Subtract output α from input I and you have the matrix $\sigma = I - \alpha$. The number k of zero elements in the matrix σ can be calculated, and then a ratio $\varepsilon = (k/n) \times 100\%$ is obtained. Under the circumstance that the matching threshold ϖ, $0 \leq \varpi \leq 1$ is set, the ratio ε, $0 \leq \varepsilon \leq 1$ is compared with the set match threshold ϖ. If the ratio $\varepsilon \geq \varpi$, it shows that this identification is successful; otherwise, it shows that this identification is a failure.

Remark 14. In the Step 1, the number of neurons of RNNs grows as more selected face images are added. The relationship between the number of neurons and the number of selected face images should satisfy the inequality: $2^n \geq m$, where n is the number of neurons of RNNs and m is the number of selected face images.

5. Experiments and Summary of Findings

In this section, recognition performance indicators are listed first. On that basis, Experiment 1 is simulated to test the feasibility of the proposed face recognition method, and Experiment 2 is simulated to evaluate the performance of the

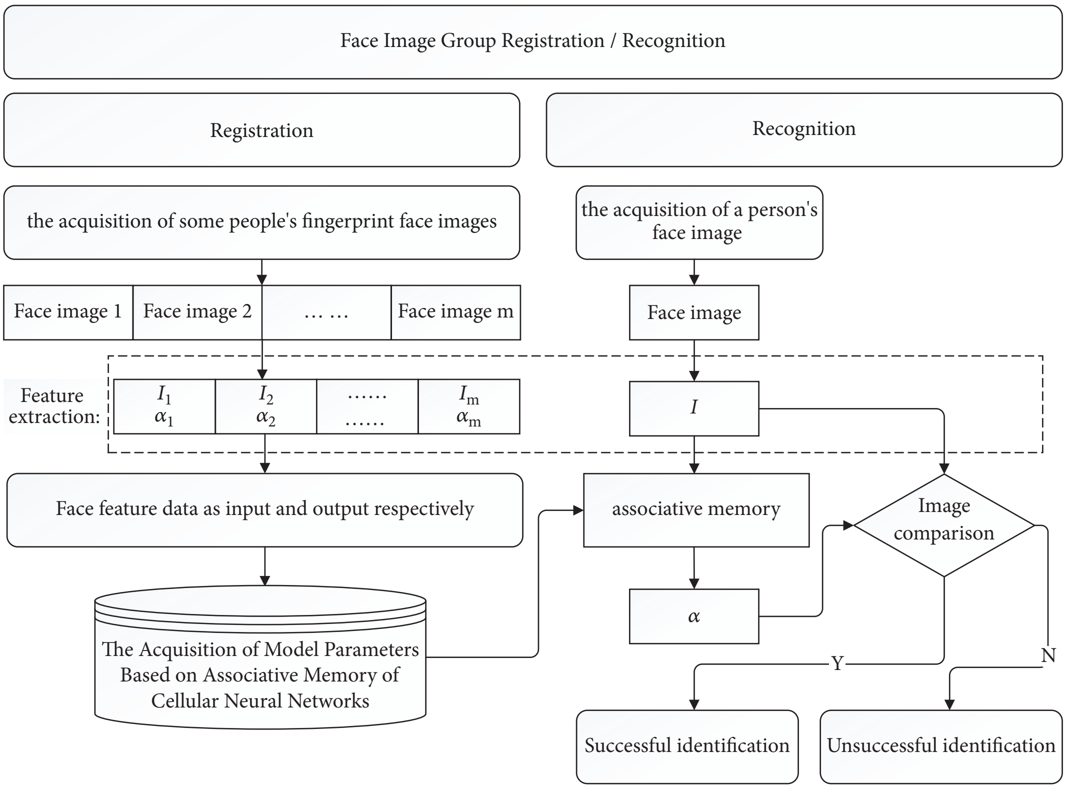

Face Image Group Registration / Recognition
Registration
Recognition
the acquisition of some people's fingerprint face images
the acquisition of a person's face image
Face image 1
Face image 2
… …
Face image m
Face image
Feature extraction:
I_1 α_1
I_2 α_2
……
I_m α_m
I
Face feature data as input and output respectively
associative memory
Image comparison
The Acquisition of Model Parameters Based on Associative Memory of Cellular Neural Networks
α
Y
N
Successful identification
Unsuccessful identification

Figure 2: Process of the face recognition method by AM based on RNNs.

proposed face recognition method. Finally, according to the results of two experiments, some findings can be summarized

5.1. Recognition Performance Indicator. In this section, the false acceptance rate (FAR) is used to evaluate the performance of the proposed face recognition method. The specific formula of FAR is as follows:

$$\mathrm{FAR} = \frac{\mathrm{NFA}}{\mathrm{TNT}} \times 100\% \tag{13}$$

where NFA and TNT stand for the number of false acceptance and the total number of tests, respectively.

From (13), we can get that lower number of FAR equate to better performance of the proposed face recognition method.

5.2. Experiment 1. Firstly, in the ORL database, selecting $m = m' \times \partial$ face images deriving from m' different people where ∂ face images are chosen for every authorized user.

According to the proposed face recognition method in Section 4, selecting $m = m' \times \partial = 4 \times 5$ face images deriving from $m' = 4$ different authorized users where $\partial = 5$ face images are chosen for every authorized user. The original pixel size of the image in the ORL database is 112×92 pixels. As shown in the Figure 3, through the size adjustment function of the Microsoft office 2010 software, the face images' size is adjusted to $n = N \times M = 33 \times 27$ pixels $= 891$ pixels. Then, the adjusted images are converted to grayscale matrixes named $I_1' = [43\ 54\ 46\ \cdots\ 36\ 31\ 30]_{33\times27}$, $I_2' = [32\ 33\ 43\ \cdots\ 36\ 34\ 37]_{33\times27}, \ldots$, and $I_{20}' = [121\ 121\ 121\ \cdots\ 80\ 79\ 81]_{33\times27}$, respectively. By setting the binary brightness threshold $\zeta = 120$, the grayscale matrixes are further transformed into binary matrixes $I_1, I_2, \ldots, I_{20}$.

The initial conditions of the established AAM model are $A = \mathrm{diag}[1, 1, \ldots, 1, \ldots, 1]_{891\times891}$, $f(\xi_i) = (1/(2 * 2))(|\xi_i + 2| - |\xi_i - 2|), i \in (1, 2, \ldots, n)$, respectively. Binary matrixes $u_1, u_2, \ldots, u_{20}$ as the input and output of the model appear as $(I_1, \alpha_1), (I_2, \alpha_2), \ldots, (I_{20}, \alpha_{20})$, respectively. According to the AAM model training method of the Step 2 in Section 4, model template parameters can be obtained $L_b{}^{(l)}, L_c{}^{(l)}, D^{(l)}$, $l \in (1, 2, \cdots 891)$.

A binary matrix

$$I = I_3 = [-1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ 1\ \ 1\ \ 1\ \ 1\ \ \cdots\ \ -1\ \ -1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0]_{33\times27} \tag{14}$$

transformed by a face image that has been trained before by AAM, is used as input to the established AAM model, then the corresponding binary output matrix can be obtained by AAM:

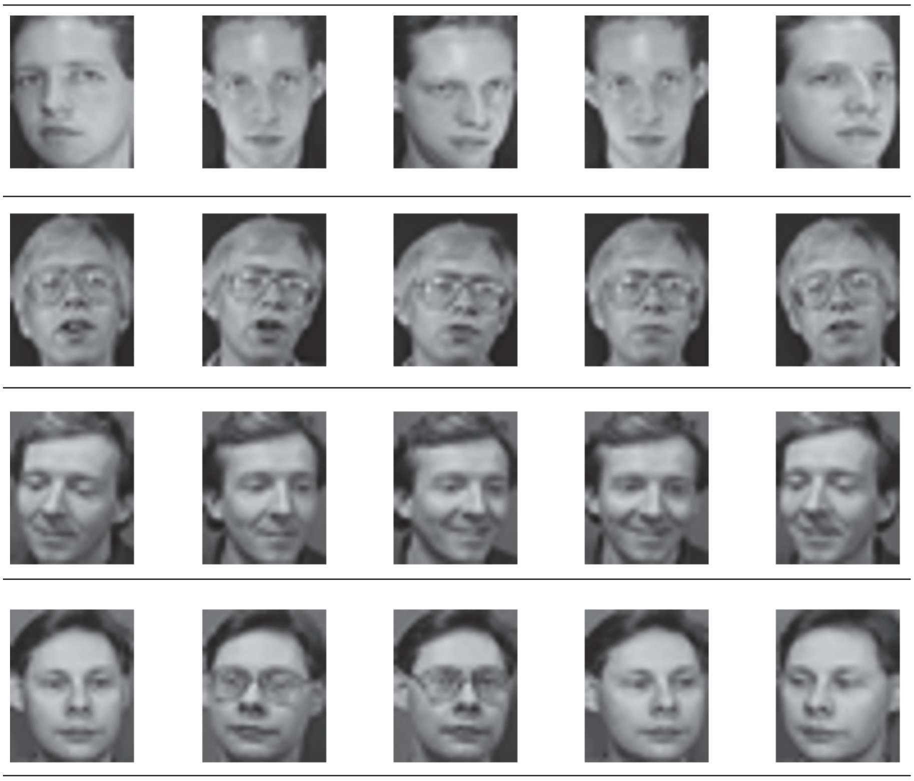


Figure 3: Dimensions adjusted face images through the size adjustment function of the Microsoft office 2010 software.

$$\alpha = \left[-1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ -1\ \ 1\ \ 1\ \ 1\ \ 1\ \ \cdots\ \ -1\ \ -1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\right]_{33\times 27}. \tag{15}$$

Subtract output α from input I and you have the matrix $\sigma = I - \alpha$. The number of zero elements in the matrix σ is $k = 891$ by calculation, and then the consistent percentage $\varepsilon = (k/n) \times 100\% = [k/(33 \times 27)] \times 100\% = 100\%$ can be obtained. If the threshold is defined as $\varpi = 0.95$, we can see that $\varepsilon = 100\% > \varpi$. Therefore, the visitor is considered to have access.

The result of experiment shows that the proposed face recognition method by AAM based on RNNs can realize biological recognition, and its feasibility is verified.

5.3. Experiment 2. According to the proposed face recognition method in Section 4, as shown in Figure 4(a), selecting $m = m' \times \partial = 2 \times 5$ face images named s1_1.bmp, s1_2.bmp, s1_3.bmp, s1_4.bmp, s1_5.bmp, s2_1.bmp, s2_2.bmp, s2_3.bmp, s2_4.bmp, and s2_5.bmp in the ORL database, respectively. Through the size adjustment function of the Microsoft office 2010 software, the face images' size is adjusted to $n = N \times M = 12 \times 9$ pixels $= 108$ pixels, and then the adjusted images are converted to grayscale matrixes named $I_1' = [47\ \ 62\ \ \cdots\ \ 49;\ \cdots;\ 44\ \ 49\ \ \cdots\ \ 26]_{12\times 9}$, $I_2' = [33\ \ 58\ \ \cdots\ \ 83;\ \cdots;\ 25\ \ 94\ \ \cdots\ \ 25]_{12\times 9}, \cdots, I_{10}' = [35\ \ 33\ \ \cdots\ \ 34;\ \cdots;\ 40\ \ 22\ \ \cdots\ \ 24]_{12\times 9}$, respectively. By setting the gray threshold $\zeta = 120$, the grayscale matrixes are further transformed into binary matrixes named $I_1, I_2, \cdots, I_{10}$, respectively.

The initial conditions of the established AAM model are $A = \operatorname{diag}[1, 1, \ldots, 1, \ldots, 1]_{891\times 891}$, $f(\xi_i) = (1/(2 \times 2))(|\xi_i + 2| - |\xi_i - 2|)$, $i \in (1, 2, \ldots, n)$, respectively. Binary matrixes $I_1, I_2, \ldots, I_{10}$ as the input and output of the model appear as $(I_1, \alpha_1), (I_2, \alpha_2), \ldots, (I_{10}, \alpha_{10})$, respectively. According to the AAM model training method of the Step 2 in Section 4, the model parameters can be obtained $L_b{}^{(l)}, L_c{}^{(l)}, D^{(l)}$, $l \in (1, 2, \ldots, 108)$.

Randomly selecting a face image which is from unregistered people, such as shown in the Figure 4(b), a face image named s5_3.bmp in the ORL database. Then, the image s5_3.bmp is transformed into a binary matrix I through the transformation of image dimension and image binarization like the processing steps in the registration phase. The binary matrix I is used as input to the established AAM model, and then the corresponding binary output matrix α can be obtained. The matrix ℓ is obtained by matrix I minus matrix

(a) The registered images of authorized user

(b) The face image of unauthorized users

Figure 4: The face images selected from the database.

α, and then the number of zero elements in the matrix $k = 95$. The consistent percentage $\varepsilon = (k/n)\times 100\% = [95/(33\times 27)]\times 100\% = 87.96\%$ can be obtained. If the threshold is defined as $\varpi = 0.95$, we can see that $\varepsilon = 87.96\% < \varpi$. Therefore, the visitor is considered to have no access.

According to the above acquired AAM model and mentioned face recognition steps, 240 face images of 24 unregistered people randomly selected from the ORL database are used as input to the established AAM model, respectively. By calculation, the false accept number is 2. Therefore, NFA = 2 and TNT = 240. Finally, according to (13), we can get that the *FAR* of the established facial recognition method is

$$\mathrm{FAR} = \frac{\mathrm{NFA}}{\mathrm{TNT}} \times 100\% = \frac{2}{240} \times 100\% = 0.83\% \tag{16}$$

The results of experiment show that if the image of an unauthorized user who is not registered before is used as input to AAM, the corresponding AAM effect is not good enough. It can be concluded that the proposed face recognition method can achieve certain face recognition effects with good performance.

5.4. Summary of Findings. In general, our findings can be summarized as follows:

(1) In the absence of a face database, the method of AAM based on RNNs can realize face recognition. That is, the AAM model based on can replace the face database to achieve the face recognition effect. Thus, the intrusion and tampering of face database are indirectly avoided.

(2) The experimental results verify the feasibility of the proposed face recognition method by AAM based on RNNs. It can guarantee that the authorized user has access; otherwise it has no access.

(3) The proposed recognition method by AAM based on RNNs not only applies to face recognition, but also applies to fingerprint identification, palm print recognition, venous recognition, etc.

6. Conclusion

In the paper, an AAM model based on RNNs is proposed to implement faces recognition in the absence of a face database. The stability of the model is studied in detail, and a design procedure of AAM is given. Based on the proposed AAM model and the procedure of AAM, a face AAM recognition method is established. Two experiments are given to verify the proposed face recognition method. From the examples in Section 5, we know that the proposed face recognition method by AAM based on RNNs is feasible.

Appendix

A.

Denote $B_k^{(i)}$ $(k = 1,2,3; i = 1,2,\ldots,N)$ as a $M \times M$ matrix. The matrix $B = (b_{ij})_{n\times n}$ $(i = 1,2,\ldots,n;\ j = 1,2,\ldots,n)$ defined by (1), composed of template has the form

$$B = \left(b_{ij}\right)_{n\times n} = \begin{bmatrix} B_2^{(1)} & B_3^{(1)} & 0 & 0 & \cdots & 0 & 0 & 0 \\ B_1^{(2)} & B_2^{(2)} & B_3^{(2)} & 0 & \cdots & 0 & 0 & 0 \\ 0 & B_1^{(3)} & B_2^{(3)} & B_3^{(3)} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & B_1^{(N-1)} & B_2^{(N-1)} & B_3^{(N-1)} \\ 0 & 0 & 0 & 0 & \cdots & 0 & B_1^{(N)} & B_2^{(N)} \end{bmatrix}_{n\times n}, \tag{A.1}$$

where

$$\begin{gathered}
B_1^{(i)} = \begin{bmatrix}
b_{(-1,0)}^{(i-1)M+1} & b_{(-1,1)}^{(i-1)M+1} & 0 & \cdots & 0 & 0 & 0 \\
b_{(-1,-1)}^{(i-1)M+2} & b_{(-1,0)}^{(i-1)M+2} & b_{(-1,1)}^{(i-1)M+2} & \cdots & 0 & 0 & 0 \\
0 & b_{(-1,-1)}^{(i-1)M+3} & b_{(-1,0)}^{(i-1)M+3} & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & b_{(-1,-1)}^{(i-1)M+(M-1)} & b_{(-1,0)}^{(i-1)M+(M-1)} & b_{(-1,1)}^{(i-1)M+(M-1)} \\
0 & 0 & 0 & 0 & 0 & b_{(-1,-1)}^{(i-1)M+M} & b_{(-1,0)}^{(i-1)M+M}
\end{bmatrix}_{M\times M}, \\
B_2^{(i)} = \begin{bmatrix}
b_{(0,0)}^{(i-1)M+1} & b_{(0,1)}^{(i-1)M+1} & 0 & \cdots & 0 & 0 & 0 \\
b_{(0,-1)}^{(i-1)M+2} & b_{(0,0)}^{(i-1)M+2} & b_{(0,1)}^{(i-1)M+2} & \cdots & 0 & 0 & 0 \\
0 & b_{(0,-1)}^{(i-1)M+3} & b_{(0,0)}^{(i-1)M+3} & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & b_{(0,-1)}^{(i-1)M+(M-1)} & b_{(0,0)}^{(i-1)M+(M-1)} & b_{(0,1)}^{(i-1)M+(M-1)} \\
0 & 0 & 0 & 0 & 0 & b_{(0,-1)}^{(i-1)M+M} & b_{(0,0)}^{(i-1)M+M}
\end{bmatrix}_{M\times M}, \\
B_3^{(i)} = \begin{bmatrix}
b_{(1,0)}^{(i-1)M+1} & b_{(1,1)}^{(i-1)M+1} & 0 & \cdots & 0 & 0 & 0 \\
b_{(1,-1)}^{(i-1)M+2} & b_{(1,0)}^{(i-1)M+2} & b_{(1,1)}^{(i-1)M+2} & \cdots & 0 & 0 & 0 \\
0 & b_{(1,-1)}^{(i-1)M+3} & b_{(1,0)}^{(i-1)M+3} & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & b_{(1,-1)}^{(i-1)M+(M-1)} & b_{(1,0)}^{(i-1)M+(M-1)} & b_{(1,1)}^{(i-1)M+(M-1)} \\
0 & 0 & 0 & 0 & 0 & b_{(1,-1)}^{(i-1)M+M} & b_{(1,0)}^{(i-1)M+M}
\end{bmatrix}_{M\times M},
\end{gathered} \tag{A.2}$$

where b_{ij} denote weight from cell j to cell i. The definition of matrix $C = (c_{ij})_{n\times n}$ $(i = 1, 2, \ldots, n;\ j = 1, 2, \ldots, n)$ is similar to B.

B. The Proof of Theorem 2

Suppose that ξ_i^* is an equilibrium point of (7). Choose $g(\xi_i) = \delta_{ii}(a_i\xi_i^* - w_i)$. Then we have

$$\begin{gathered} -a_i\xi_i(t) + b_{ii}\alpha_i + w_i = 0. \\ \delta_{ii}\left(a_i\xi_i^* - w_i\right) = \alpha_i. \end{gathered} \tag{B.1}$$

(I) If $\xi_i^* > h, \alpha_i = \lambda$. Thus, we have

$$\delta_{ii}\left(a_i\xi_i^* - w_i\right) = \lambda. \tag{B.2}$$

Then, we have

$$\frac{\lambda + \delta_{ii}w_i}{\delta_{ii}a_i} = \xi_i^* \geq h. \tag{B.3}$$

Therefore, from $0 < \delta_{ii}a_i \leq \lambda/h$ and $a_i > 0$, we have $w_i \geq a_ih - \lambda/\delta_{ii}$.

Define $g(\xi_i) = \delta_{ii}(a_i\xi_i - w_i)$. From Figure 5, it is obvious that when $g(\xi_i) = \lambda$, $\xi_i^* > h$, ξ_i^* is a positive equilibrium point of (7).

(II) If $\xi_i^* < -h, \alpha_i = -\lambda$. Thus, we have

$$\delta_{ii}\left(a_i\xi_i^* - w_i\right) = \alpha_i = -\lambda. \tag{B.4}$$

Then, we have

$$\frac{-\lambda + \delta_{ii}w_i}{\delta_{ii}a_i} = \xi_i^* \leq -h. \tag{B.5}$$

Therefore, from $0 < \delta_{ii}a_i \leq \lambda/h$ and $a_i < 0$, we have $w_i \leq \lambda/\delta_{ii} - a_ih$.

From Figure 6, it is obvious that when $g(\xi_i) = -1$ and $\xi_i^* < -h$, ξ_i^* is a negative equilibrium point of (7).

C.

Choose $l \in (1, 2, \ldots, n)$, $k \in (1, 2, \ldots, m)$, $q \in (1, 2, \ldots, N)$, $n = N \times M$,

$$\begin{gathered}
B' = \operatorname{diag}\left(b_{(0,0)}^{1}, b_{(0,0)}^{2}, \ldots, b_{(0,0)}^{n}\right), \\
L_b{}^{(l)} = \left[b_{(-1,-1)}^{(l)}, b_{(-1,0)}^{(l)}, b_{(-1,1)}^{(l)}, b_{(0,-1)}^{(l)}, 0, b_{(0,1)}^{(l)}, b_{(1,-1)}^{(l)}, b_{(1,0)}^{(l)}, \right. \\
\left. b_{(1,1)}^{(l)}\right]_{9\times 1}^{T}, \\
L_b = \left[L_b{}^{(1)}, L_b{}^{(2)}, \ldots, L_b{}^{(n)}\right]_{n\times 9}^{T};
\end{gathered}$$

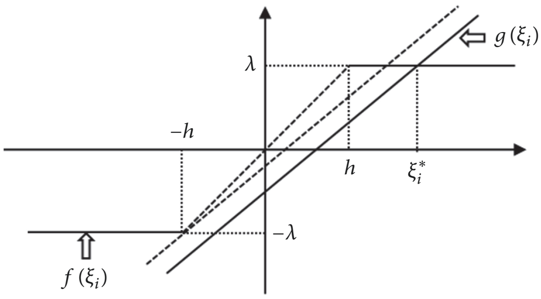


Figure 5: When $0 < \delta_{ii}a_i \leq \lambda/h$ and $g(\xi^*_{\,i}) = f(\xi_i^*)$, $\xi_i^* \geq h, \xi_i^*$ is a positive equilibrium point of (7).

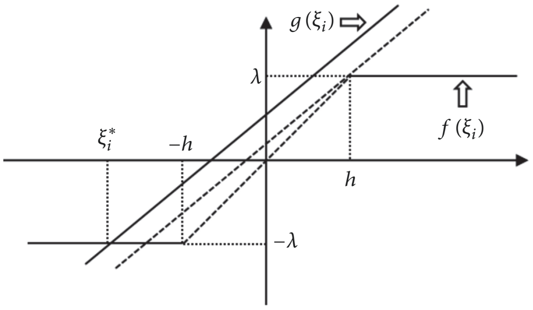


Figure 6: When $0 < \delta_{ii}a_i \leq \lambda/h$ and $g(\xi^*_{\,i}) = f(\xi_i^*)$, $\xi_i^* \leq -h, \xi_i^*$ is a negative equilibrium point of (7).

$$L_c^{(l)} = \left[c^{(l)}_{(-1,-1)}, c^{(l)}_{(-1,0)}, c^{(l)}_{(-1,1)}, c^{(l)}_{(0,-1)}, c^{(l)}_{(0,0)}, c^{(l)}_{(0,1)}, c^{(l)}_{(1,-1)}, c^{(l)}_{(1,0)}, c^{(l)}_{(1,1)}\right]^T_{9\times 1},$$

$$L_c = \left[L_c^{(1)}, L_c^{(2)}, \ldots, L_c^{(n)}\right]^T_{n\times 9};$$

$$D = \left(D^{(1)}, D^{(2)}, \ldots, D^{(l)}, \ldots, D^{(n)},\right)^T_{n\times 1},$$

$$L^{(l)}_{con} = \left(\left(L_b^{(l)}\right)^T, \left(L_c^{(l)}\right)^T, D^{(l)}\right)^T_{19\times 1}.$$

$$\Upsilon = \left(\alpha_1, \alpha_2, \ldots, \alpha_k, \ldots, \alpha_m\right)_{n\times m},$$

$$\alpha_k = \left(\alpha_k^{(1)}, \alpha_k^{(2)}, \ldots, \alpha_k^{(l)}, \ldots, \alpha_k^{(n)}\right)^T_{n\times 1},$$

$$\widehat{\Upsilon} = \left(\left(\alpha_1\right)^T, \left(\alpha_2\right)^T, \ldots, \left(\alpha_m\right)^T\right)^T_{nm\times 1},$$

$$\widehat{\Upsilon}^{(l)} = \left(\alpha_1^{(l)}, \alpha_2^{(l)}, \ldots, \alpha_m^{(l)}\right)^T_{m\times 1};$$

$$I' = \left(I_1, I_2, \ldots, I_m\right)_{n\times m},$$

$$I_k = \left(I_k^{(1)}, I_k^{(2)}, \ldots, I_k^{(n)}\right)^T_{n\times 1},$$

$$I = \left(\left(I_1\right)^T, \left(I_2\right)^T, \ldots, \left(I_m\right)^T\right)_{nm\times 1};$$

$$\mathrm{T}_k^q = \begin{bmatrix} 0 & I_k^{(q-1)M+1} & I_k^{(q-1)M+2} \\ I_k^{(q-1)M+1} & I_k^{(q-1)M+2} & I_k^{(q-1)M+3} \\ I_k^{(q-1)M+2} & I_k^{(q-1)M+3} & I_k^{(q-1)M+4} \\ \vdots & \vdots & \vdots \\ I_k^{qM-2} & I_k^{qM-1} & I_k^{qM} \\ I_k^{qM-1} & I_k^{qM} & 0 \end{bmatrix}_{M\times 3},$$

$$\mathrm{T}_k = \begin{bmatrix} 0 & \mathrm{T}_k^1 & \mathrm{T}_k^2 \\ \mathrm{T}_k^1 & \mathrm{T}_k^2 & \mathrm{T}_k^3 \\ \mathrm{T}_k^2 & \mathrm{T}_k^3 & \mathrm{T}_k^4 \\ \vdots & \vdots & \vdots \\ \mathrm{T}_k^{N-2} & \mathrm{T}_k^{N-1} & \mathrm{T}_k^N \\ \mathrm{T}_k^{N-1} & \mathrm{T}_k^N & 0 \end{bmatrix}_{n\times 9},$$

$$\mathrm{T} = \begin{bmatrix} \mathrm{T}_1 \\ \mathrm{T}_2 \\ \vdots \\ \mathrm{T}_k \\ \vdots \\ \mathrm{T}_m \end{bmatrix}_{nm\times 9},$$

$$\mathrm{T}_k = \left(\mathrm{T}_k^{(1)}, \mathrm{T}_k^{(2)}, \ldots, \mathrm{T}_k^{(n)}\right)^T_{n\times 9},$$

$$\mathrm{T}^{(l)} = \left(\left(\mathrm{T}_1^{(l)}\right)^T, \left(\mathrm{T}_2^{(l)}\right)^T, \ldots, \left(\mathrm{T}_m^{(l)}\right)^T\right)^T_{m\times 9},$$

$$\Theta_k^q = \begin{bmatrix} 0 & \alpha_k^{(q-1)M+1} & \alpha_k^{(q-1)M+2} \\ \alpha_k^{(q-1)M+1} & \alpha_k^{(q-1)M+2} & \alpha_k^{(q-1)M+3} \\ \alpha_k^{(q-1)M+2} & \alpha_k^{(q-1)M+3} & \alpha_k^{(q-1)M+4} \\ \vdots & \vdots & \vdots \\ \alpha_k^{qM-2} & \alpha_k^{qM-1} & \alpha_k^{qM} \\ \alpha_k^{qM-1} & \alpha_k^{qM} & 0 \end{bmatrix}_{M\times 3},$$

$$\Theta_k = \begin{bmatrix} 0 & \Theta_k^1 & \Theta_k^2 \\ \Theta_k^1 & \Theta_k^2 & \Theta_k^3 \\ \Theta_k^2 & \Theta_k^3 & \Theta_k^4 \\ \vdots & \vdots & \vdots \\ \Theta_k^{N-2} & \Theta_k^{N-1} & \Theta_k^N \\ \Theta_k^{N-1} & \Theta_k^N & 0 \end{bmatrix}_{n\times 9},$$

$$\Theta = \begin{bmatrix} \Theta_1 \\ \Theta_2 \\ \vdots \\ \Theta_k \\ \vdots \\ \Theta_m \end{bmatrix}_{nm\times 9},$$

$$\begin{aligned}
&\Theta_k = \left(\Theta_k^{(1)}, \Theta_k^{(2)}, \ldots, \Theta_k^{(n)}\right)_{n\times 9}^T, \\
&\Theta^{(l)} = \left(\Theta_1^{(l)}, \Theta_2^{(l)}, \ldots, \Theta_k^{(l)}, \ldots, \Theta_m^{(l)}\right)_{m\times 9}^T, \\
&\Theta' = (0, 0, 0, 0, \widehat{\Upsilon}, 0, 0, 0, 0)_{nm\times 9}, \\
&\Theta_k' = (0, 0, 0, 0, \alpha_k, 0, 0, 0, 0)_{n\times 9} \\
&\mathrlap{-}\Theta = \Theta - \Theta' = (\mathrlap{-}\Theta_1, \mathrlap{-}\Theta_2, \ldots, \mathrlap{-}\Theta_m)_{nm\times 9}^T, \\
&\Theta = \Theta_k - \Theta_k' \\
&\Theta^{(l)} = \left(\left(\mathrlap{-}\Theta_1^{(l)}\right)^T, \left(\mathrlap{-}\Theta_2^{(l)}\right)^T, \ldots, \left(\mathrlap{-}\Theta_m^{(l)}\right)^T\right)_{m\times 9}^T \\
&\widehat{\Theta}^{(q)} = \left(\mathrlap{-}\Theta_q^T, \mathrlap{-}\Theta_{n+q}^T, \ldots, \mathrlap{-}\Theta_{(m-1)n+q}^T\right)_{m\times 9}^T, \\
&e = [1, 1, \ldots, 1]_{m\times 1}^T, \\
&\Delta^{(l)} = \left[\Xi^{(l)}, \Theta^{(l)}, e\right]_{m\times 19}, \\
&\Delta = \left(\left(\Delta^{(1)}\right)^T, \left(\Delta^{(2)}\right)^T, \ldots, \left(\Delta^{(n)}\right)^T\right)_{19\times nm}.
\end{aligned} \tag{C.1}$$

D.

Proof. Let $\Lambda^{(l)} = (\lambda \mathrlap{-}\Theta^{(l)}, \mathrm{T}^{(l)}, e)$ and $\psi^{(l)} = \eta \widehat{\Upsilon}^{(l)}$,

From (12), we have

$$\begin{aligned}
&\left\|\Lambda^{(l)} L_{con}^{(l)} - \psi^{(l)}\right\|_2^2 = \left\|\Lambda^{(l)} L_{con}^{(l)} - \psi^{(l)}\right. \\
&\quad \left. + \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)} - \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)}\right\|_2^2 \\
&\quad = \left[\Lambda^{(l)} L_{con}^{(l)} - \psi^{(l)} + \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)}\right. \\
&\quad \left. - \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)}\right]^T \left[\Lambda^{(l)} L_{con}^{(l)} - \psi^{(l)}\right. \\
&\quad \left. + \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)} - \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)}\right] \\
&\quad = \left\|\Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\omega^{(l)} - \psi^{(l)}\right\|_2^2 + \left\|\Lambda^{(l)} L_{con}^{(l)}\right. \\
&\quad \left. - \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)}\right\|_2^2 + \left[\Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)}\right. \\
&\quad \left. - \psi^{(l)}\right]^T \cdot \left[\Lambda^{(l)} L_{con}^{(l)} - \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)}\right] \\
&\quad + \left[\Lambda^{(l)} L_{con}^{(l)} - \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)}\right]^T \\
&\quad \cdot \left[\Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)} - \psi^{(l)}\right],
\end{aligned} \tag{D.1}$$

where

$$\begin{aligned}
&\left[\Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)} - \psi^{(l)}\right]^T \\
&\quad \cdot \left[\Lambda^{(l)} L_{con}^{(l)} - \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)}\right] = \left(\psi^{(l)}\right)^T \\
&\quad \cdot \left[\Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\right]^T \Lambda^{(l)} L_{con}^{(l)} - \left(\psi^{(l)}\right)^T \\
&\quad \cdot \left[\Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\right]^T \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)} - \left(\psi^{(l)}\right)^T \\
&\quad \cdot \Lambda^{(l)} L_{con}^{(l)} + \left(\psi^{(l)}\right)^T \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)} = \left(\psi^{(l)}\right)^T \\
&\quad \cdot \Lambda^{(l)} L_{con}^{(l)} - \left(\psi^{(l)}\right)^T \Lambda^{(l)} L_{con}^{(l)} + \left(\psi^{(l)}\right)^T \\
&\quad \cdot \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)} - \left(\psi^{(l)}\right)^T \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)} \\
&\quad = 0.
\end{aligned} \tag{D.2}$$

Then

$$\begin{aligned}
&\left[\Lambda^{(l)} L_{con}^{(l)} - \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)}\right]^T \\
&\times \left[\Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)} - \psi^{(l)}\right] \\
&\quad = \left\{\left[\Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\omega^{(l)} - \psi^{(l)}\right]^T\right. \\
&\quad \left. \times \left[\Lambda^{(l)} L_{con}^{(l)} - \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)}\right]\right\}^T = 0.
\end{aligned} \tag{D.3}$$

Therefore,

$$\begin{aligned}
&\left\|\Lambda^{(l)} L_{con}^{(l)} - \psi^{(l)}\right\|_2^2 = \left\|\Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)} - \psi^{(l)}\right\|_2^2 \\
&\quad + \left\|\Lambda^{(l)} L_{con}^{(l)} - \Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)}\right\|_2^2 \\
&\quad \geq \left\|\Lambda^{(l)} pinv\left(\Lambda^{(l)}\right)\psi^{(l)} - \psi^{(l)}\right\|_2^2.
\end{aligned} \tag{D.4}$$

It is obvious that $L_{con}^{(l)} = pinv(\lambda \mathrlap{-}\Theta^{(l)}, \mathrm{T}^{(l)}, e)\lambda \widehat{\Upsilon}^{(l)}$ is least square solution of (12). □

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Qi Han, Zhengyang Wu, Shiqin Deng, and Jin Liu made the same contribution to the work and should be considered co-first authors.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (61503050, 51374268, and 51275547), in part by the Key Technology Project for Heavy Accident Prevention and Control of Safe Production in 2018 (Chongqing-0004-2018AQ), in part by the Program of Chongqing Fundamental and Frontier Research Plan (cstc2017jcyjAX0115 and cstc2018jcyjAX0583), in part by the Foundation of Chongqing University of Education (KY201702A), in part by the graduate science and technology innovation program of Chongqing University of Science & Technology (YKJCX1720407), and in part by the Chongqing Outstanding Youth Fund Project (cstc2014jcyjjq90002). Thanks are due to Doctor Yaping He of the School of Computing, Engineering and Mathematics, Western Sydney University, for the review and revision.

References

[1] D. Zhang, *Automated Biometrics: Technologies and Systems*, Springer Science & Business Media, 2013.

[2] A. Lumini and L. Nanni, "Overview of the combination of biometric matchers," *Information Fusion*, vol. 33, pp. 71–85, 2017.

[3] A. Ross, K. Nandakumar, A. Jain, Handbook of Multibiometrics, 6, Springer, 2006.

[4] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[5] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Biometrics break-ins and band-aids," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2105–2113, 2003.

[6] A. Kong, D. Zhang, and M. Kamel, "Three measures for secure palmprint identification," *Pattern Recognition*, vol. 41, no. 4, pp. 1329–1337, 2008.

[7] *ISO/IEC 24745 Information Technology, Security techniques, Biometric information protection*, 2010.

[8] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on Homomorphic Encryption," *Pattern Recognition*, vol. 67, pp. 149–163, 2017.

[9] S. Wang and J. Hu, "A blind system identification approach to cancelable fingerprint templates," *Pattern Recognition*, vol. 54, pp. 14–22, 2016.

[10] S. Wang, W. Yang, and J. Hu, "Design of Alignment-Free Cancelable Fingerprint Templates with Zoned Minutia Pairs," *Pattern Recognition*, vol. 66, pp. 295–301, 2017.

[11] H. Kaur and P. Khanna, "Gaussian Random Projection Based Non-invertible Cancelable Biometric Templates," in *Proceedings of the 11th International Conference on Communication Networks, ICCN 2015*, pp. 661–670, India, August 2015.

[12] G. Amirthalingam and G. Radhamani, "New chaff point based fuzzy vault for multimodal biometric cryptosystem using particle swarm optimization," *Journal of King Saud University - Computer and Information Sciences*, vol. 28, no. 4, pp. 381–394, 2016.

[13] M. Lafkih, M. Mikram, S. Ghouzali, M. El Haziti, and D. Aboutajdine, "Biometric cryptosystems based fuzzy commitment scheme: A security evaluation," *International Arab Journal of Information Technolog*, vol. 13, no. 4, pp. 443–449, 2016.

[14] Y. Imamverdiyev, A. B. J. Teoh, and J. Kim, "Biometric cryptosystem based on discretized fingerprint texture descriptors," *Expert Systems with Applications*, vol. 40, no. 5, pp. 1888–1901, 2013.

[15] A. C.-C. Yao, "How to generate and exchange secrets," in *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*, pp. 162–167, Toronto, Canada, October 1986.

[16] M. Barni, G. Droandi, and R. Lazzeretti, "Privacy Protection in Biometric-Based Recognition Systems: A marriage between cryptography and signal processing," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 66–76, 2015.

[17] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 88–100, 2015.

[18] C. Zhou, X. Zeng, H. Jiang, and L. Han, "A generalized bipolar auto-associative memory model based on discrete recurrent neural networks," *Neurocomputing*, vol. 162, pp. 201–208, 2015.

[19] Z. Zeng and J. Wang, "Design and analysis of high-capacity associative memories based on a class of discrete-time recurrent neural networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 38, no. 6, pp. 1525–1536, 2008.

[20] Q. Han, X. Liao, T. Huang, J. Peng, C. Li, and H. Huang, "Analysis and design of associative memories based on stability of cellular neural networks," *Neurocomputing*, vol. 97, pp. 192–200, 2012.

[21] Z. Wang, H. Zhang, and B. Jiang, "LMI-based approach for global asymptotic stability analysis of recurrent neural networks with various delays and structures," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 22, no. 7, pp. 1032–1045, 2011.

[22] Z. Wang, L. Liu, Q.-H. Shan, and H. Zhang, "Stability criteria for recurrent neural networks with time-varying delay based on secondary delay partitioning method," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 26, no. 10, pp. 2589–2595, 2015.

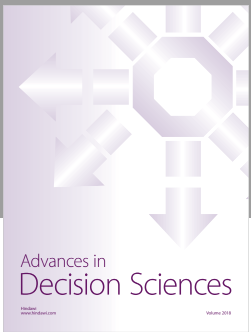
[23] Z. Wang, S. Ding, Q. Shan, and H. Zhang, "Stability of recurrent neural networks with time-varying delay via flexible terminal method," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 28, no. 10, pp. 2456–2463, 2017.

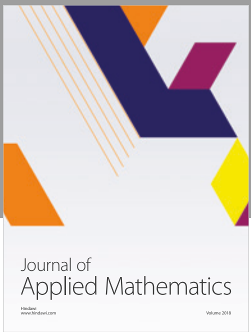
[24] X. He, C. Li, T. Huang, C. Li, and J. Huang, "A recurrent neural network for solving bilevel linear programming problem," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 25, no. 4, pp. 824–830, 2014.

[25] X. He, T. Huang, J. Yu, C. Li, and C. Li, "An inertial projection neural network for solving variational inequalities," *IEEE Transactions on Cybernetics*, vol. 47, no. 3, pp. 809–814, 2017.

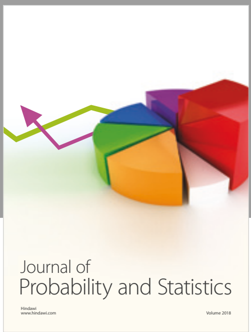
[26] D. Liu and A. N. Michel, "Cellular Neural Networks for Associative Memories," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 40, no. 2, pp. 119–121, 1993.

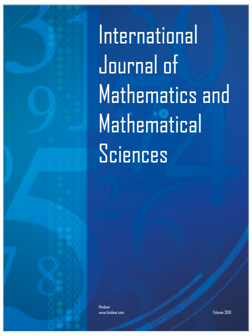
Advances in
Operations Research


Advances in
Decision Sciences

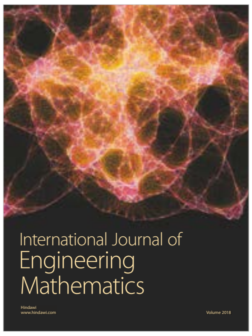

Journal of
Applied Mathematics

The Scientific
World Journal

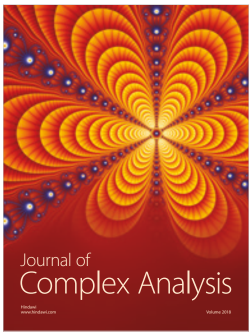

Journal of
Probability and Statistics

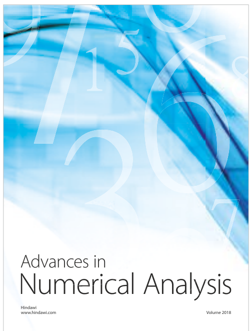

International
Journal of
Mathematics and
Mathematical
Sciences

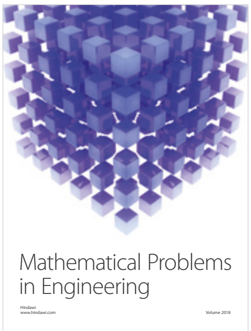
Journal of
Optimization

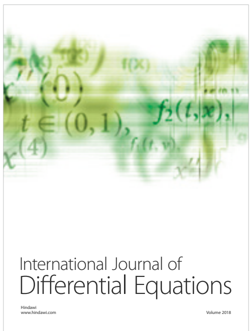

International Journal of
Engineering
Mathematics

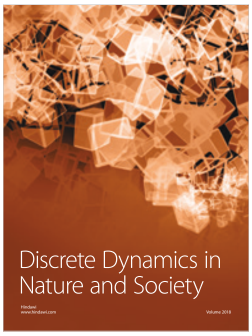
International Journal of
Analysis

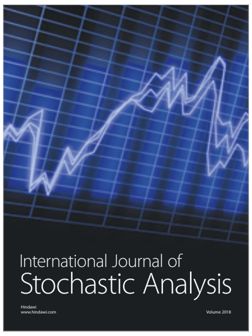

Journal of
Complex Analysis


Advances in
Numerical Analysis


Mathematical Problems
in Engineering

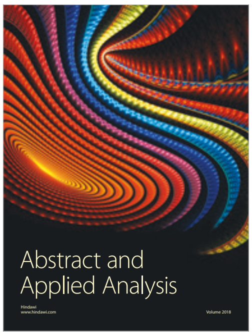

International Journal of
Differential Equations

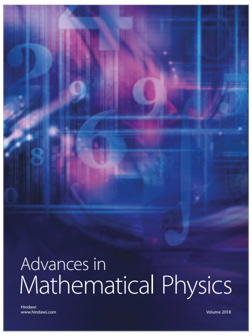

Discrete Dynamics in
Nature and Society


International Journal of
Stochastic Analysis

Journal of
Mathematics

Journal of
Function Spaces


Abstract and
Applied Analysis


Advances in
Mathematical Physics