

Article

# Multimodal Identification Based on Fingerprint and Face Images via a Hetero-Associative Memory Method

Qi Han <sup>1</sup>, Heng Yang <sup>1,\*</sup>, Tengfei Weng <sup>2</sup>, Guorong Chen <sup>1</sup>, Jinyuan Liu <sup>1</sup> and Yuan Tian <sup>1</sup>

<sup>1</sup> College of Intelligent Technology and Engineering, Chongqing University of Science and Technology, Chongqing 401331, China; hanqicq@163.com (Q.H.); cgr@cqust.edu.cn (G.C.); yjhqqqidri@126.com (J.L.); tianyuan@cqu.edu.cn (Y.T.)

<sup>2</sup> College of Electrical Engineering, Chongqing University of Science and Technology, Chongqing 401331, China; wengtf\_cq@163.com

\* Correspondence: yh@cqust.edu.cn

**Abstract:** Multimodal identification, which exploits biometric information from more than one biometric modality, is more secure and reliable than unimodal identification. Face recognition and fingerprint recognition have received a lot of attention in recent years for their unique advantages. However, how to integrate these two modalities and develop an effective multimodal identification system are still challenging problems. Hetero-associative memory (HAM) models store some patterns that can be reliably retrieved from other patterns in a robust way. Therefore, in this paper, face and fingerprint biometric features are integrated by the use of a hetero-associative memory method for multimodal identification. The proposed multimodal identification system can integrate face and fingerprint biometric features at feature level when the system converges to the state of asymptotic stability. In experiment 1, the predicted fingerprint by inputting an authorized user's face is compared with the real fingerprint, and the matching rate of each group is higher than the given threshold. In experiment 2 and experiment 3, the predicted fingerprint by inputting the face of an unauthorized user and the stealing authorized user's face is compared with its real fingerprint input, respectively, and the matching rate of each group is lower than the given threshold. The experimental results prove the feasibility of the proposed multimodal identification system.

**Keywords:** stability; multimodal identification; fingerprint recognition; face recognition



check for updates

**Citation:** Han, Q.; Yang, H.; Weng, T.; Chen, G.; Liu, J.; Tian, Y. Multimodal Identification Based on Fingerprint and Face Images via a Hetero-Associative Memory Method.

*Mathematics* **2021**, *9*, 2976.

<https://doi.org/10.3390/math9222976>

Academic Editor:

Ezequiel López-Rubio

Received: 28 October 2021

Accepted: 16 November 2021

Published: 22 November 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

With the rapid development of science and technology, people pay more attention to security identification than ever before, and new theories and technologies continually emerge for identity authentication. Traditional identification methods include key, password, code, identification card, and so on. One of the weaknesses of these methods is that unauthorized persons can fabricate or steal protected data and make use of the rights of authorized users to engage in illegal activities. Though these traditional identification technologies, which usually face various threats in real world, are still playing an indispensable role on various occasions with a low request of security for their convenience and low cost, increasingly more consumers and enterprises choose to use biometric identification in numerous fields. Biometric identification technologies such as face recognition [1–4], fingerprint recognition [5–7], and gait recognition [8–10] are more secure and convenient than traditional technologies.

Biometric identification refers to the automated recognition of individuals based on their biological or behavioral characteristics [11]. It is closely combined with high-tech means such as optics, acoustics, biosensors, and biostatistics. Biometrics finds its applications in the following areas: access control to facilities and computers, criminal identification, border security, access to nuclear power plants, identity authentication in network environment, airport security, issue of passports or driver licenses, and forensic

and medical databases [12]. Biometric identification can facilitate a well-rounded solution for system identification and maintain a reliable and secure system. Biometric technology has started to become a booming field and an important application direction of a cross subject between computer science and biology. Unimodal biometric systems, such as fingerprint identification system and face identification, have been studied in many previous articles [6,13–20].

Through the studies of recent years, it is evident that multimodal biometric identification technologies that use many kinds of biometric characteristics to identify individuals are more secure and accurate than unimodal ones. They take advantage of multiple biometric traits to improve the performance in many aspects including accuracy, noise resistance, universality, and spoof attacks, and reduce performance degradation in huge database applications [21]. Multi-biometric feature fusion is a crucial step in multimodal biometric systems. The strength of the feature fusion technique lies in its ability to derive highly discriminative information from original multiple feature sets and to eliminate redundant information that results from the correlation between distinct feature sets, thus gaining the most effective feature set with low dimensionality for the final decision [22]. On the process of multimodal identification research, several new algorithms and applications have been studied in recent years. For example, the authors of [11] presented a multimodal biometric approach based on the fusion of the finger vein and electrocardiogram (ECG) signals. The application of canonical correlation analysis (CCA) in multimodal biometric field attracted many researchers [23,24], who employed CCA to fuse gait and face cues for human gender recognition. Multimodal biometric identification system based on finger geometry, knuckle print, and palm print was proposed in [21]. Face–iris multimodal biometric system using a multi-resolution Log–Gabor filter with spectral regression kernel discriminant analysis was studied in [25]. The authors of [26] proposed an efficient multimodal face and fingerprint biometrics authentication system on space-limited tokens, e.g., smart cards, driver license, and RFID cards. The authors of [27] proposed a novel multimodal biometric identification system for face–iris recognition, based on binary particle swarm optimization and solving the problem of mutually exclusive redundant features in combined features. Dialog Communication Systems (DCS AG) developed BioID in [28], a multimodal identification system that uses three different features—face, voice, and lip movement—to identify people. In [29], a frequency-based approach results in a homogeneous biometric vector, integrating iris and fingerprint data. The authors of [30] proposed a deep multimodal fusion network to fuse multiple modalities (face, iris, and fingerprint) for person identification. They demonstrate an increase in multimodal person identification performance by utilizing the proposed multi-level feature abstract representations in our multimodal fusion, rather than using only the features from the last layer of each modality-specific CNN. However, the system in [30] based on CNNs cannot be used for small samples.

Associative memory networks are single layer nets that can store and recall patterns based on data content rather than data address [31]. Associative memory (AM) systems can be divided into hetero-associative memory (HAM) systems and auto-associative memory (AAM) systems. When the input pattern and the output pattern are the same pattern, the system can be called an AAM system. The HAM model, which stores coupling information based on input–output patterns, can recall a stored output pattern by receiving a different input pattern. In [32], to protect the face features database fundamentally, a new face recognition method by AAM based on RNNs is proposed without establishing a face feature database, in which the face features are transformed into the parameters of the AAM model. We notice that the HAM models can construct the association between the input and output patterns in a robust way, and this association can be regarded as feature fusion of two different kinds of patterns. Thus, HAM models should be able to fuse multiple biometric features in a robust way. Furthermore, the multimodal identification system can be built by HAM models.

Considering the advantages of multimodal identification and the fusion capability of HAM models, in this paper, the HAM model, which can store fusion features of face–

fingerprint patterns and recall a predictable fingerprint pattern by receiving a face pattern, is constructed. The model is based on a cellular neural network, which belongs to a class of recurrent neural networks (RNNs). The stability of the HAM model is a prerequisite for its successful application in a multimodal identification system. Thus, the asymptotic stability of the HAM model is also analyzed and discussed. In this paper, we also propose a multimodal identification system based on fingerprint and face images by the HAM method. Our three contributions in this paper are highlighted as follows.

- A multimodal identification system based on face and fingerprint images is designed, and this system effectively utilizes the advantages of two representative biometric features and ensures the system more security in the process of identification.
- The variable gradient method is used to construct the Lyapunov function, which proves the asymptotic stability of the HAM model. The HAM model based on RNNs must converge to the asymptotic equilibrium point. Otherwise, multimodal identification cannot be carried out in practical scenarios. Analyses and discussions of the stability are given.
- This is the first attempt to integrate face and fingerprint biometric features using the HAM method. In the HAM model, fingerprint and face biometric features are fused in a robust way. All the biometric features are fused to form a set of model coupling parameters.

The remainder of this paper is organized as follows. In Sections 2 and 3, we give the details of our proposed multimodal identification system and research background, respectively. In Section 4, the stability of the HAM model is analyzed in detail and the main results for feature fusion are given. Some numerical simulations are presented to illustrate the effectiveness and security of the proposed system in Section 5. Finally, some conclusions are drawn in Section 6.

## 2. Framework of the Identification System

We design a multimodal identification system based on face and fingerprint images that makes full use of the advantages of two different biometric modalities. We put forward two stages, which are named the fusion stage and identification stage in this identification system. The framework of the proposed system is shown in Figure 1.

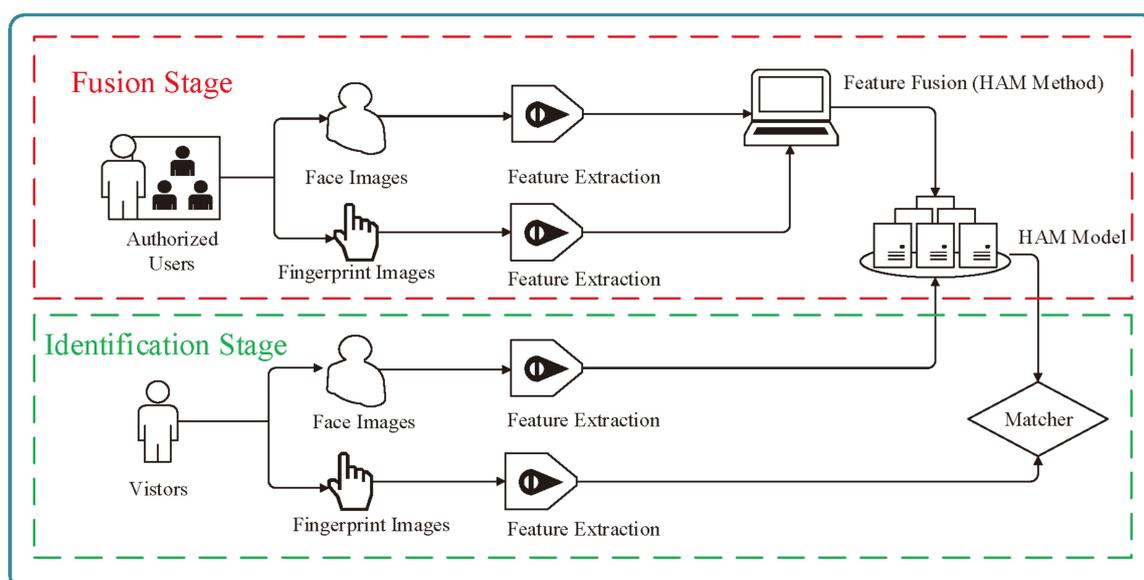


Figure 1. The framework of the multimodal identification system.

At the fusion stage, the main work is to establish the HAM model, which stores information of feature fusion using the HAM method. The HAM model, which is used for feature fusion, is based on an improved HAM method, and the established model can store the coupling information of the face and fingerprint patterns of the authorized users. The first step is to acquire face images and fingerprint images of the authorized users using some feature extractor device. The raw images are preprocessed, including the processes of gray level transformation, image binarization, and segmentation. The regions of interest (ROIs) of face images and fingerprint images after preprocessing are used to fuse both face and fingerprint biometric features using the HAM method. The parameters that come from the feature fusion institute crucial model coefficients of the HAM model. Then, the established HAM model can recall the fingerprint pattern of one authorized user by receiving the face pattern of the user when the model converges to the asymptotically stable equilibrium point. If the established model could not converge to the asymptotically stable equilibrium point, the fusion parameters, namely model coefficients, would not be given. The HAM model stores two kinds of biometric features of all authorized users as one group of model coefficients, and those biometrical features cannot be decrypted easily in the reversible method.

In the identification stage, the HAM model established in the fusion stage is used to test the legitimacy of the visitors. Firstly, the face image and fingerprint image of one visitor are acquired using proper feature extractor devices in the identification stage. The visitor’s face pattern after preprocessing is sent to the HAM model established in the fusion stage. Then, there will be an output pattern when the established HAM model converges to the asymptotically stable equilibrium point. By comparing the model’s output pattern with the visitor’s real fingerprint pattern after preprocessing, the recognition pass rate of the visitor can be obtained. If the numerical value of the recognition rate of the visitor exceeds a given threshold, the identification is successful and the visitor has the rights of authorized users. Instead, the visitor is an illegal user.

### 3. Research Background

In this section, we briefly introduce the HAM model, which is based on a class of recurrent neural networks, as well as the background knowledge of the system stability and variable gradient method.

#### 3.1. HAM Model

Consider a class of recurrent neural network composed of  $N$  rows and  $M$  columns with time-varying delays as

$$\dot{s}_i(t) = -p_i s_i(t) + \sum_{j=1}^n q_{ij} f(s_j(t)) + \sum_{j=1}^n r_{ij} u_j(t - \tau_{ij}(t)) + v_i, i = (1, 2, \dots, n) \quad (1)$$

in which  $n$  corresponds to the number of neurons in the neural network and  $n = N \times M$   $s_i(t) \in R$  is the state of the  $i$ th neuron at time  $t$ ;  $p_i > 0$  represents the rate with which the  $i$ th unit will reset its potential to the resting state in isolation when disconnected from the network and external inputs;  $q_{ij}$  and  $r_{ij}$  are connection weights;  $f(s_j(t)) = (|s_j(t) + 1| - |s_j(t) - 1|)/2$  is an activation function;  $u_j$  is the neuron input;  $\tau_{ij}$  is the transmission delay, which is the time delay between the  $i$ th neuron and the  $j$ th neuron in the network;  $v_i$  is an offset value of the  $i$ th neuron; and  $i = 1, 2, \dots, n$ .

For one neuron, we can obtain the equation of dynamics as (1). Nevertheless, when considering the whole neural network, (1) can be expressed as

$$\dot{s} = -Ps + Qf(s) + R\beta + V \quad (2)$$

in which  $s = (s_1, s_2, \dots, s_n)^T \in R^n$  is a neuron network state vector;  $P = \text{diag}(p_1, p_2, \dots, p_n) \in R_+^n$  is a positive parameter diagonal matrix;  $f(s)$  is  $n$  dimensions vector whose value changes between  $-1$  and  $+1$ ; and  $\beta_{n \times 1}$  is the network input vector whose value is  $-1$  or

+1, especially, when the neural network comes to the state of global asymptotic stability, let  $\alpha = f(s^*) \in \{\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)^T \mid \alpha_i = +1 \text{ or } -1, i = 1, \dots, n\}$ .  $V = (v_1, v_2, \dots, v_n)^T$  denotes an offset value vector.  $Q, R$ , and  $V$  are the model parameters.  $Q_{n \times n}$  and  $R_{n \times n}$  are denoted as the connection weights matrix of the neuron network as follows

$$Q = \begin{pmatrix} q_{11} & q_{12} & \dots & q_{1n} \\ q_{21} & q_{22} & \dots & q_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ q_{n1} & q_{n2} & \dots & q_{nn} \end{pmatrix}_{n \times n} \quad R = \begin{pmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ r_{21} & r_{22} & \dots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \dots & r_{nn} \end{pmatrix}_{n \times n}$$

### 3.2. System Stability

Consider the general nonlinear system

$$\dot{y} = g(t, y) \tag{3}$$

in which  $y = (y_1, y_2, \dots, y_n) \in \Omega \subseteq R^n$  is a state vector;  $t \in I = [t_0, T]$  is a time variable,  $t_0 < T < \infty$ . Then,  $g(t, y) = [g_1(t, y_1, \dots, y_n), g_2(t, y_1, \dots, y_n), \dots, g_n(t, y_1, \dots, y_n)]^T$  and  $g(t, y) \in C(I \times \Omega, R^n)$ . Supposing that  $y = \varphi(t)$  is a special solution of system (3). Let  $y = x + \varphi(t)$ , then  $\dot{x} = \dot{y} - \dot{\varphi}(t) = g(t, y) - g[t, \varphi(t)] = g[t, x + \varphi(t)] - g[t, \varphi(t)]$ . Let  $\dot{x} = f(t, x)$ , then the system (3) can be rewritten as

$$\dot{x} = f(t, x) \tag{4}$$

**Definition 1.** If  $x_0$  satisfies  $f(t, x_0) \equiv 0, 0 \leq t_0 \leq t$ , then  $x_0$  is the equilibrium point of system (4).

**Definition 2.**  $x_0$  is the equilibrium point of system (4). If, for any given  $\epsilon > 0$  and  $t_0 > 0$ , there exists  $\sigma(\epsilon, t_0) > 0$ , when  $x_1 \in R^n$  satisfies  $\|x_1 - x_0\| \leq \sigma$  such that  $\|\varphi(t, t_0, x_1) - x_0\| \leq \epsilon$ . Then, the equilibrium point  $x_0$  of Equation (4) is said to be stable in the sense of Lyapunov stability theory. Furthermore, if  $\lim_{x \rightarrow \infty} \|\varphi(t, t_0, x_1) - x_0\| = 0$ , then the equilibrium point  $x_0$  is asymptotically stable.

### 3.3. Variable Gradient Method

The most challenging problem for which to use Lyapunov’s second method (direct method) is to find a positive definite function  $V$  that yields  $\dot{V} < 0$ . The variable gradient method, which was proposed by Scultz, is one of the famous techniques for constructing a Lyapunov function to prove the stability of nonlinear systems [33]. The idea of this method is to construct the gradient of the Lyapunov function to analyze the sign property of Lyapunov function.

For the nonlinear system (4), if there exists the Lyapunov function  $V(x) : D \rightarrow R, D \subseteq R^n, V(x)$  is an explicit function of  $x$ , and the equilibrium point of the system is the origin, i.e.,  $x^* = 0$ , the single value gradient  $gradV$  of  $V(x)$  can be defined as

$$gradV(x) \triangleq \frac{dV(x)}{dx} = \begin{pmatrix} \partial V / \partial x_1 \\ \partial V / \partial x_2 \\ \vdots \\ \partial V / \partial x_n \end{pmatrix} = \begin{pmatrix} \nabla V_1 \\ \nabla V_2 \\ \vdots \\ \nabla V_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \dots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \dots + a_{2n}x_n \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + a_{n3}x_3 + \dots + a_{nn}x_n \end{pmatrix} \tag{5}$$

It follows from (5) that

$$\dot{V}(x) = \sum_{i=1}^n \left( \frac{\partial V}{\partial x_i} \cdot \dot{x}_i \right) = (gradV(x))^T [\dot{x}_1, \dots, \dot{x}_n]^T = (gradV(x))^T \dot{x} \tag{6}$$

It can be seen from (6) that  $V(x)$  can be obtained by the line integral of  $gradV$ , namely,

$$V(x) = \int_0^x (gradV)^T dx = \int_0^x \sum_{i=1}^n x_i \nabla V_i dx_i \tag{7}$$

If  $n$ -dimensional curl of  $gradV$  is equal to zero, namely,  $rot(gradV) = 0$ , then  $V$  can be regarded as a conservative field, and the line integral shown in the above formula (7) is independent of the path. The necessary and sufficient condition for  $rot(gradV) = 0$  is  $\partial \nabla V_i / \partial x_j = \partial \nabla V_j / \partial x_i, \forall i, j = 1, 2, \dots, n$ . Therefore, for convenience, Formula (7) can be rewritten as

$$V(x) = \int_0^{x_1} \nabla V_1 \Big|_{(x_1, 0, \dots, 0)} dx_1 + \int_0^{x_2} \nabla V_2 \Big|_{(x_1, x_2, 0, \dots, 0)} dx_2 + \dots + \int_0^{x_n} \nabla V_n \Big|_{(x_1, x_2, x_3, \dots, x_n)} dx_n \tag{8}$$

By selecting appropriate coefficients such that  $\dot{V}(x)$  is negative definite and  $rot(gradV)$  is equal to zero. If  $V(x)$  is positive definite, then the second method of Lyapunov is proved, and the system is asymptotically stable at the equilibrium point.

#### 4. Main Results

In this section, under the research background, the asymptotic stability of the HAM model with multiple time-varying delays using variable gradient method and the algorithm of feature fusion by the HAM method are presented successively.

##### 4.1. Stability of the HAM Model

**Theorem 1.** *There is a stable equilibrium point in system (2), which makes the HAM model asymptotically stable.*

**Proof of Theorem 1.** As  $f$  is bounded, it can be proved that system (2) has at least one equilibrium point using Schauder fixed point theorem. Assuming that  $s^* = (s_1^*, s_2^*, \dots, s_n^*)^T$  is an equilibrium point in the neural network.

Let  $x_i(t) = s_i(t) - s_i^*$  and  $\bar{f}(x_i(t)) = f(s_i(t)) - f(s_i^*) = f(x_i(t) + s_i^*) - f(s_i^*)$ , then (1) can be rewritten as

$$\begin{cases} \dot{x}_i(t) = -p_i x_i(t) + \sum_{j=1}^n q_{ij} \bar{f}(x_j(t)) + \sum_{j=1}^n r_{ij} u_j(t - \tau_{ij}(t)) + c_i \\ c_i = \sum_{j=1}^n q_{ij} f(s_j^*) - p_i s_i^* + v_i, \quad i = (1, 2, \dots, n) \end{cases} \tag{9}$$

For the HAM model (9), if there exist the Lyapunov function  $V(x)$ , and the model's equilibrium point is  $x^* = (x_1^*, x_2^*, \dots, x_n^*)^T = 0$ , the single value gradient of (9) can be defined as Equation (5). From Equation (6),

$$\begin{aligned} \dot{V}(x) &= (gradV(x))^T \dot{x} \\ &= (a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n)\dot{x}_1 + \dots + (a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n)\dot{x}_n \end{aligned} \tag{10}$$

It is convenient to select coefficients  $a_{ij} = 0, (i \neq j)$  and  $a_{kk} > 0, i, j, k = 1, 2, \dots, n$  from (9), and one can easily obtain

$$\begin{aligned} \dot{V}(x) &= a_{11}x_1\dot{x}_1 + \dots + a_{nn}x_n\dot{x}_n = \sum_{k=1}^n a_{kk}x_k\dot{x}_k \\ &= \sum_{k=1}^n \left( a_{kk}x_k(t) \left( -p_k x_k(t) + \sum_{j=1}^n q_{kj} \bar{f}(x_j(t)) + \sum_{j=1}^n r_{kj} u_j(t - \tau_{kj}(t)) + c_k \right) \right) \end{aligned} \tag{11}$$

When  $\dot{s}_k = 0$ , from Equation (1),  $s_k^* = \left( \sum_{j=1}^n q_{kj}f(s_j(t)) + \sum_{j=1}^n r_{kj}u_j(t - \tau_{kj}(t)) + v_k \right) / p_k$ .  
 If  $x_k(t) > 0$ , i.e.,  $s_k(t) - s_k^* > 0$ , then  $p_k s_k(t) > \sum_{j=1}^n q_{kj}f(s_j(t)) + \sum_{j=1}^n r_{kj}u_j(t - \tau_{kj}(t)) + v_k$ . By replacing  $s_k(t)$  with  $x_k(t)$ , the inequality  $-p_k x_k(t) + \sum_{j=1}^n q_{kj}\bar{f}(x_j(t)) + \sum_{j=1}^n r_{kj}u_j(t - \tau_{kj}(t)) + c_k < 0$  can be obtained. Analogously, if  $x_k(t) < 0$ , it can be proved that  $-p_k x_k(t) + \sum_{j=1}^n q_{kj}\bar{f}(x_j(t)) + \sum_{j=1}^n r_{kj}u_j(t - \tau_{kj}(t)) + c_k > 0$ . Therefore, both cases can lead to  $\dot{V}(x) < 0$ , namely  $\dot{V}(x)$  is negative definite. Furthermore, it is clear that  $\partial \nabla V_i / \partial x_j = \partial \nabla V_j / \partial x_i = 0, \forall i, j = 1, 2, \dots, n$ . Therefore, from Equation (8), the Lyapunov function can be obtained as

$$\begin{aligned} V(x) &= \int_0^{x_1} \nabla V|_{(x_1, 0, \dots, 0)} dx_1 + \int_0^{x_2} \nabla V|_{(x_1, x_2, 0, \dots, 0)} dx_2 + \dots + \int_0^{x_n} \nabla V|_{(x_1, x_2, \dots, x_n)} dx_n \\ &= \int_0^{x_1} a_{11}x_1 dx_1 + \int_0^{x_2} (a_{21}x_1 + a_{22}x_2) dx_2 + \dots + \int_0^{x_n} (a_{n1}x_1 + \dots + a_{nn}x_n) dx_n \\ &= \int_0^{x_1} a_{11}x_1 dx_1 + \int_0^{x_2} a_{22}x_2 dx_2 + \dots + \int_0^{x_n} a_{nn}x_n dx_n \end{aligned} \tag{12}$$

which is always positive definite. Then, we proved the HAM model is asymptotically stable at the equilibrium point using the variable gradient method. □

**Remark 1.** The HAM method is used to fuse each authorized user’s face and fingerprint biometric features. The face and fingerprint patterns of each authorized user are the input vector  $\beta_{n \times 1} = [\beta_1, \beta_2, \dots, \beta_n]^T$  and output vector  $\alpha_{n \times 1} = [\alpha_1, \alpha_2, \dots, \alpha_n]^T$  of the neural network model, respectively. When the established HAM model converges to the asymptotically stable equilibrium point, the output vector can be obtained by receiving an input vector, i.e., the fingerprint pattern can be recalled by the face pattern of the authorized user.

#### 4.2. HAM Model

The HAM method is used to fuse each authorized user’s face and fingerprint biometric features. The authorized user’s face and fingerprint patterns are the network model’s input vector  $\beta_{n \times 1}$  and output vector  $\alpha_{n \times 1}$ , respectively.

Letting  $f(s_j(t)) = \hat{\alpha}_j, |\hat{\alpha}_j| \leq 1, \beta_j = u_j(t - \tau_{ij}(t)), \beta \in \{(\beta_1, \beta_2, \dots, \beta_n)^T | \beta_j = +1 \text{ or } -1, i = 1, \dots, n\}$ , Equation (1) can be rewritten as

$$\dot{s}_i(t) = -p_i s_i(t) + \sum_{j=1}^n q_{ij} \hat{\alpha}_j + \sum_{j=1}^n r_{ij} \beta_j + v_i \tag{13}$$

**Lemma 1 ([34]).** In Equation (13),  $s_i(0) = 0, i = 1, 2, \dots, n$ ,

(i) If  $\sum_{j=1}^n q_{ij} \hat{\alpha}_j + \sum_{j=1}^n r_{ij} \beta_j + v_i > p_i$ , then (13) can converge to an asymptotically stable equilibrium point whose value is greater than +1.

(ii) If  $\sum_{j=1}^n q_{ij} \hat{\alpha}_j + \sum_{j=1}^n r_{ij} \beta_j + v_i < -p_i$ , then (13) can converge to an asymptotically stable equilibrium point whose value is less than -1.

**Theorem 2.** HAM model (2) converges to a stable equilibrium point  $s^*$  and  $|s^*| > 1$ , if there exists a constant  $\lambda$  such that  $\lambda \geq \max_{1 \leq i \leq n} \{p_i\}$  and  $Q\alpha + R\beta + V = \lambda\alpha$ .

**Proof of Theorem 2.** In (2),  $s^* = [s_1^*, s_2^*, \dots, s_n^*]^T$ . Define the equilibrium of the HAM model  $s^* = [s_1^*, s_2^*, \dots, s_n^*]^T, \alpha = f(s^*) \in \{\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)^T | \alpha_i = +1 \text{ or } -1\}$  is an equilibrium point in the neural network.

For the first case, consider  $\alpha_i = +1$ , then  $\lambda\alpha_i > p_i$ . When  $Q\alpha + R\beta + V = \lambda\alpha$ , according to Lemma 1 (i),  $\sum_{j=1}^n q_{ij}\alpha_j + \sum_{j=1}^n r_{ij}\beta_j + v_i > p_i$ . For the second case, consider  $\alpha_i = -1$ , then  $\lambda\alpha_i < -p_i$ . When  $Q\alpha + R\beta + V = \lambda\alpha$ , according to Lemma 1 (ii),  $\sum_{j=1}^n q_{ij}\alpha_j + \sum_{j=1}^n r_{ij}\beta_j + v_i < -p_i$ . Therefore, the HAM model (2) converges to a stable equilibrium point  $s^*$ , where  $|s^*| > 1$ .  $\square$

Given  $S = \alpha$  and  $U = \beta$ , in which  $\alpha$  and  $\beta$  are the feature vectors extracted from the fingerprint and face images of one authorized user after preprocessing, respectively.

It is obvious that, when  $\alpha$  and  $\beta$  meet the condition in Theorem 2, the coupling relationship of the face and fingerprint patterns of one authorized user is established, and the fusion features are transformed into HAM model parameters. The HAM model, which stores fusion features of face and fingerprint patterns of the user, can recall a predictable fingerprint pattern  $\hat{S}$  by receiving a stored face pattern  $U$ . The HAM model network is of size  $N \times M$ . Let the neighborhood radius be 1, then there are eighteen unknown connection weights and one unknown bias value  $v_i$  for one neuron. Denote the nineteen unknown parameters of the  $i$ th neuron as  $\Phi_i = [q_{i-1}, q_{i-2}, \dots, q_{i-8}, q_{i-9}, r_{i-1}, r_{i-2}, \dots, r_{i-8}, r_{i-9}, v_i]^T$ .

**Remark 2.** In the fusion stage, the established HAM model can store fusion features of all authorized users. Therefore, all model parameters  $\Phi_i (i = 1, 2, \dots, n)$  to be obtained should be determined by the face and fingerprint patterns of all authorized users.

For  $m$  authorized users,  $Q\alpha + R\beta + V = \lambda\alpha$  can be transformed as

$$\Delta_i \Phi_i = \tilde{\alpha}_i \lambda \quad (i = 1, 2, \dots, n) \tag{14}$$

$$\text{in which } \Delta_i = \begin{pmatrix} \alpha_{i1}^{(1)} & \alpha_{i2}^{(1)} & \dots & \alpha_{i9}^{(1)} & \beta_{i1}^{(1)} & \beta_{i2}^{(1)} \dots & \beta_{i9}^{(1)} & 1 \\ \alpha_{i1}^{(2)} & \alpha_{i2}^{(2)} & \dots & \alpha_{i9}^{(2)} & \beta_{i1}^{(2)} & \beta_{i2}^{(2)} \dots & \beta_{i9}^{(2)} & 1 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{i1}^{(m-1)} & \alpha_{i2}^{(m-1)} & \dots & \alpha_{i9}^{(m-1)} & \beta_{i1}^{(m-1)} & \beta_{i2}^{(m-1)} \dots & \beta_{i9}^{(m-1)} & 1 \\ \alpha_{i1}^{(m)} & \alpha_{i2}^{(m)} & \dots & \alpha_{i9}^{(m)} & \beta_{i1}^{(m)} & \beta_{i2}^{(m)} \dots & \beta_{i9}^{(m)} & 1 \end{pmatrix}$$

and  $\tilde{\alpha}_i = [\alpha_i^1, \alpha_i^2, \dots, \alpha_i^m]^T$  is the fingerprint pattern's feature vector of  $m$  authorized users on the  $i$ -th neuron of the network model.

Then, all unknown model parameters by Equation (14) can be solved. Namely, two kinds of biometric features of all authorized users turn into parameters of the established HAM. After obtaining all the parameters based on face and fingerprint patterns of all authorized users, the HAM model, which can recall fingerprint pattern by receiving the face pattern of the authorized user, is established.

Some notations are defined in Appendix A. The feature fusion algorithm of the HAM model based on face and fingerprint images using the HAM method in the fusion stage is given in Algorithm 1.

**Remark 3.** When the established HAM model, which stores biometric fusion features of all authorized users, receives a face pattern vector of an unauthorized user, there will exist a forecasting fingerprint pattern output of the visitor. In [32], the input pattern and forecasting output pattern are the same biometric pattern. It uses the AAM network structure, which fuses the face input and the same face output, but it cannot achieve the fusion of different biological models. In this paper, two different biometric patterns are studied. This is the first attempt to integrate two different biometric features using the HAM method.

Furthermore, the convolutional neural network needs a lot of data for training, which is difficult to train for small samples, so we do not use the convolutional neural network for small sample data in this paper.

---

**Algorithm 1** Feature fusion algorithm
 

---

**Require:**  $\lambda \geq \max_{1 \leq i \leq n} \{p_i\}$  fingerprint feature vector  $\alpha^{(k)}$ , face feature vector  $\beta^{(k)}$ ,  $k = 1, 2, \dots, m$ .  
**Ensure:** Model parameters  $\Phi_i, i = 1, 2, \dots, n$ .  
**for**  $k = 1 \rightarrow m$  **do**  
**for**  $\xi = 1 \rightarrow N$  **do**  
 $E_\xi^{(k)} \leftarrow \alpha^{(k)}, F_\xi^{(k)} \leftarrow \beta^{(k)}$   
**end for**  
 $E^{(k)} \leftarrow E_\xi^{(k)}, F^{(k)} \leftarrow F_\xi^{(k)}$   
**end for**  
**for**  $i = 1 \rightarrow n$  **do**  
 $\Delta_i \leftarrow E^{(1)}, E^{(2)}, \dots, E^{(m)}, F^{(1)}, F^{(2)}, \dots, F^{(m)}$   
**end for**  
**for**  $i = 1 \rightarrow n$  **do**  
**for**  $k = 1 \rightarrow m$  **do**  
 $\tilde{\alpha}_i \leftarrow \alpha^{(k)}$   
**end for**  
**end for**  
**for**  $i = 1 \rightarrow n$  **do**  
 $\Phi_i = \Delta_i^{-1} \tilde{\alpha}_i \lambda$   
**end for**

---

## 5. Experiments and Discussion

In this section, we will show the experimental results of the multimodal identification system we proposed in Section 2. Firstly, we prove the effectiveness of the multimodal identification system using Experiment 1. The accuracy of the experiment meets the requirement of identification recognition that we defined. Secondly, we test unauthorized users and prove the security of the multimodal identification system using Experiment 2.

To protect private information, the experiments are based on two different public databases. The face images come from ORL Faces Database and the fingerprint images come from CASIA-FingerprintV5 Database. The fingerprint images of CASIA-FingerprintV5 were captured by a URU4000 fingerprint sensor in one session.

In order to compare the result of the fingerprint pattern  $\tilde{S}$  of the visitor and the predictable fingerprint pattern  $\hat{S}$ , a matcher is designed. The pass rate (PR) of the matcher is defined as

$$\text{PR} = \frac{\text{NF}}{M \times N} \times 100\%$$

in which NF stands for the number of feature points that satisfy the value of the fingerprint pattern of the visitor and the predicted fingerprint output is equal in corresponding pixel coordinate. When the value of PR is bigger than the given threshold of 90%, the face pattern and the fingerprint patterns of the visitor are regarded as legal. Namely, the real fingerprint pattern of the visitor can match the predicted fingerprint output in the multimodal identification system.

### 5.1. Experiment 1

We assume that the face image and fingerprint image in each group come from the same person. Seven groups of images of authorized users from two databases mentioned above are shown in Figure 2. The first step in the biometric identification system is to extract region of interests (ROIs). In our experiments, all face image ROIs and fingerprint image ROIs used in our experiments after preprocessing are  $35 \times 25$  pixels in size.

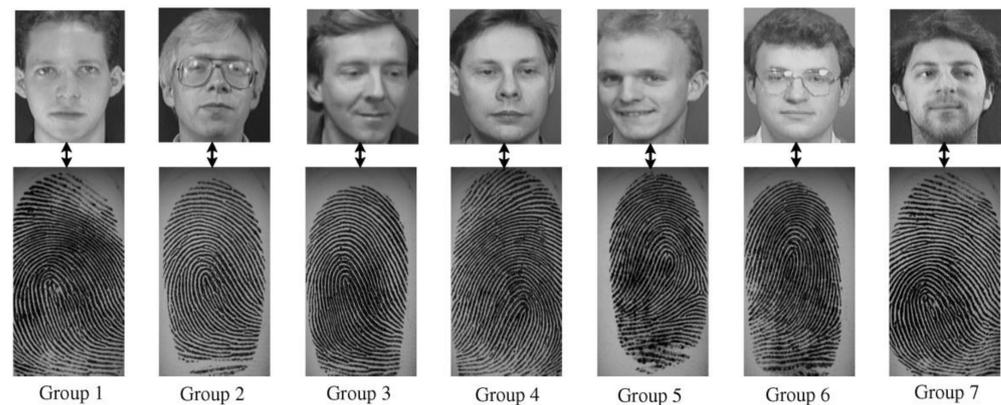


Figure 2. Seven groups of biometric images of authorized users.

The seven groups of face patterns and fingerprint patterns are used to solve the model parameters  $\Phi_i (i = 1, 2, \dots, 875)$ . Let  $p_i = 1 (i = 1, 2, \dots, 875)$  and  $\lambda = 2$ . The fingerprint feature vectors  $(\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(7)})$  and the face feature vectors  $(\beta^{(1)}, \beta^{(2)}, \dots, \beta^{(7)})$  can be obtained from the seven groups of face patterns and fingerprint patterns of all authorized users.  $E_1^{(1)}, E_2^{(1)}, \dots, E_{35}^{(1)}, E_1^{(2)}, E_2^{(2)}, \dots, E_{35}^{(2)}, \dots, E_1^{(7)}, E_2^{(7)}, \dots, E_{35}^{(7)}$  and  $F_1^{(1)}, F_2^{(1)}, \dots, F_{35}^{(1)}, F_1^{(2)}, F_2^{(2)}, \dots, F_{35}^{(2)}, \dots, F_1^{(7)}, F_2^{(7)}, \dots, F_{35}^{(7)}$  were obtained by face feature vectors and fingerprint feature vectors, respectively. According to the feature fusion algorithm, the matrix  $\Delta_1, \dots, \Delta_{875}$  was obtained. Furthermore,  $\hat{\alpha}_1, \hat{\alpha}_2, \dots, \hat{\alpha}_{875}$  was obtained through the matrix transform method. Finally,  $\Phi_i (i = 1, 2, \dots, 875)$  was calculated using the matrix operation.

According to the proposed HAM method in Section 4, when the unestablished HAM model comes to the asymptotic stable equilibrium point, the internal coupling relationship between face and fingerprint patterns will be built by solving the model parameters.

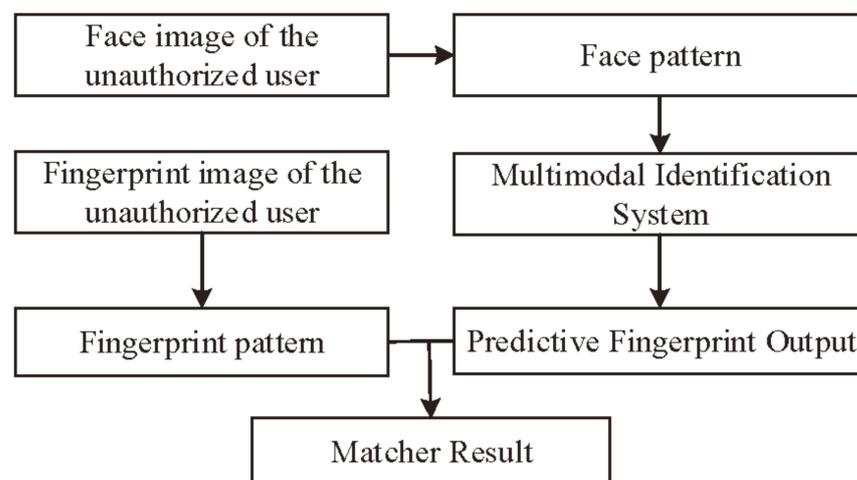
The established multimodal identification system fused face and fingerprint biometrics in the fusion stage. The matcher pass rate can be obtained by comparing  $\tilde{S}$  and  $\hat{S}$  when the system input is one of the face patterns of the authorized users. We testified the matcher pass rate as shown in Table 1, whose results prove the effectiveness of the multimodal identification system.

Table 1. The recognition pass rate of the multimodal identification system for authorized users.

Group ID	PR (%)	Pass Threshold (%)	Matcher Result (Y/N)
Group 1	96.00	90.00	Y
Group 2	93.37	90.00	Y
Group 3	96.11	90.00	Y
Group 4	93.03	90.00	Y
Group 5	94.51	90.00	Y
Group 6	92.46	90.00	Y
Group 7	96.34	90.00	Y

### 5.2. Experiment 2

The results of the experiment above test the feasibility and efficiency of the algorithm. Provided that an unauthorized user has access to the identification system, the matcher pass rate must be low enough for the system to reject illegal users. In this experiment, we choose seven groups of unauthorized users whose fingerprints and faces are different from the groups in Experiment 1. The flow diagram of identification is shown in Figure 3.



**Figure 3.** Seven groups of biometric images of authorized users (The flow diagram).

In this experiment, we found that the pass rate of unauthorized users is much lower than the identification matcher threshold. Hence, those users who attempted to spoof this identification system were identified as illegal users. We obtained seven groups of unauthorized users' identification results, shown in Table 2.

**Table 2.** The matcher pass rate of the multimodal identification system for unauthorized users.

Group ID	PR (%)	Pass Threshold (%)	Matcher Result (Y/N)
Group 8	66.86	90.00	N
Group 9	69.03	90.00	N
Group 10	68.00	90.00	N
Group 11	67.43	90.00	N
Group 12	70.86	90.00	N
Group 13	72.11	90.00	N
Group 14	68.11	90.00	N

Consider the case wherein attacker who has the forged fingerprint or the forged face of one authorized user through illegal means beforehand wants to cheat the system. As the illegal attacker completely hacked one kind of biometrical information, it is easy to cheat single-mode identification system if there is no extra validation. However, in the multimodal identification system, the attacker cannot spoof this identification system easily. Group 15 to Group 21 are the attackers who have face information of the authorized users (Group 1 to Group 7), respectively. Further, Group 22 to Group 28 are the attackers who have fingerprint information of the authorized users (Group 1 to Group 7), respectively. The identification results are shown in Table 3. The results of the experiment proved the security of our proposed system.

The experiment results prove the feasibility of the proposed multimodal identification system based on the HAM method. It can guarantee that the authorized users have access, while the unauthorized users and attackers have no access. The proposed identification method by fusing two different biometric modalities based on the HAM method applies not only to the situation of fusing the face and fingerprint feature, but also to other different biometric modalities.

**Table 3.** The matcher pass rate of the multimodal identification system for unauthorized users.

Group ID	PR (%)	Pass Threshold (%)	Matcher Result (Y/N)
Group 15	73.94	90.00	N
Group 16	80.69	90.00	N
Group 17	78.17	90.00	N
Group 18	75.66	90.00	N
Group 19	73.14	90.00	N
Group 20	73.49	90.00	N
Group 21	72.23	90.00	N
Group 22	76.57	90.00	N
Group 23	72.57	90.00	N
Group 24	71.09	90.00	N
Group 25	73.49	90.00	N
Group 26	74.63	90.00	N
Group 27	76.11	90.00	N
Group 28	71.77	90.00	N

## 6. Conclusions

To solve the multimodal identification problem based on face and fingerprint images, in this paper, we proposed a new feature fusion method for multimodal identification based on the HAM model, which can well fuse face features and fingerprint features of the authorized users. In the process of constructing the multimodal identification system, the stability of the established network model is discussed. We prove that the HAM model can reach the asymptotically stable state when the HAM model fuses face and fingerprint biometrics. The proposed multimodal identification system can integrate face and fingerprint biometric features at feature level when the system converges to the state of asymptotic stability. In Section 5, we test the effectiveness and security of the proposed multimodal identification system based on face and fingerprint images using two experiments.

**Author Contributions:** Conceptualization, Q.H. and H.Y.; methodology, H.Y.; software, T.W.; validation, G.C.; formal analysis, J.L.; investigation, Y.T.; writing—original draft preparation, H.Y.; writing—review and editing, Q.H.; visualization, H.Y.; supervision, Q.H. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded in part by CAS “Light of West China” Program, in part by Research Foundation of The Natural Foundation of Chongqing City (cstc2021jcyj-msxmX0146), in part by Scientific and Technological Research Program of Chongqing Municipal Education Commission (KJZD-K201901504, KJQN 201901537), in part by humanities and social sciences research of Ministry of Education (19YJCZH047), and in part by Postgraduate Innovation Program of Chongqing University of Science and Technology (YKJCX2020820). The authors would like to thank the support of China Scholarship Council.

**Informed Consent Statement:** All the images and data used in this article were taken from public repositories.

**Data Availability Statement:** The data used to support the findings of this study are available from the corresponding author.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Appendix A

$$E_{\xi}^{(k)} = \begin{pmatrix} 0 & \alpha_{(\xi-1)M+1}^{(k)} & \alpha_{(\xi-1)M+2}^{(k)} \\ \alpha_{(\xi-1)M+1}^{(k)} & \alpha_{(\xi-1)M+2}^{(k)} & \alpha_{(\xi-1)M+3}^{(k)} \\ \alpha_{(\xi-1)M+2}^{(k)} & \alpha_{(\xi-1)M+3}^{(k)} & \alpha_{(\xi-1)M+4}^{(k)} \\ \vdots & \vdots & \vdots \\ \alpha_{\xi M-2}^{(k)} & \alpha_{\xi M-1}^{(k)} & \alpha_{\xi M}^{(k)} \\ \alpha_{\xi M-1}^{(k)} & \alpha_{\xi M}^{(k)} & 0 \end{pmatrix}_{M \times 3} \quad E^{(k)} = \begin{pmatrix} 0 & E_1^{(k)} & E_2^{(k)} \\ E_1^{(k)} & E_2^{(k)} & E_3^{(k)} \\ E_2^{(k)} & E_3^{(k)} & E_4^{(k)} \\ \vdots & \vdots & \vdots \\ E_{N-1}^{(k)} & E_N^{(k)} & 0 \end{pmatrix}_{n \times 9}$$

$$F_{\xi}^{(k)} = \begin{pmatrix} 0 & \beta_{(\xi-1)M+1}^{(k)} & \beta_{(\xi-1)M+2}^{(k)} \\ \beta_{(\xi-1)M+1}^{(k)} & \beta_{(\xi-1)M+2}^{(k)} & \beta_{(\xi-1)M+3}^{(k)} \\ \beta_{(\xi-1)M+2}^{(k)} & \beta_{(\xi-1)M+3}^{(k)} & \beta_{(\xi-1)M+4}^{(k)} \\ \vdots & \vdots & \vdots \\ \beta_{\xi M-2}^{(k)} & \beta_{\xi M-1}^{(k)} & \beta_{\xi M}^{(k)} \\ \beta_{\xi M-1}^{(k)} & \beta_{\xi M}^{(k)} & 0 \end{pmatrix}_{M \times 3} \quad F^{(k)} = \begin{pmatrix} 0 & F_1^{(k)} & F_2^{(k)} \\ F_1^{(k)} & F_2^{(k)} & F_3^{(k)} \\ F_2^{(k)} & F_3^{(k)} & F_4^{(k)} \\ \vdots & \vdots & \vdots \\ F_{N-1}^{(k)} & F_N^{(k)} & 0 \end{pmatrix}_{n \times 9}$$

## References

1. Wang, S.-H.; Phillips, P.; Dong, Z.-C.; Zhang, Y.-D. Intelligent facial emotion recognition based on stationary wavelet entropy and Jaya algorithm. *Neurocomputing* **2018**, *272*, 668–676. [\[CrossRef\]](#)
2. Zhang, Y.-D.; Yang, Z.-J.; Lu, H.; Zhou, X.-X.; Phillips, P.; Liu, Q.-M.; Wang, S. Facial Emotion Recognition Based on Biorthogonal Wavelet Entropy, Fuzzy Support Vector Machine, and Stratified Cross Validation. *IEEE Access* **2016**, *4*, 8375–8385. [\[CrossRef\]](#)
3. Lawrence, S.; Giles, C.L.; Tsoi, A.C.; Back, A.D. Face recognition: A convolutional neural-network approach. *IEEE Trans. Neural Netw.* **1997**, *8*, 98–113. [\[CrossRef\]](#)
4. Tan, X.; Triggs, W. Enhanced Local Texture Feature Sets for Face Recognition Under Difficult Lighting Conditions. *IEEE Trans. Image Process.* **2010**, *19*, 1635–1650. [\[CrossRef\]](#)
5. Barni, M.; Scotti, F.; Piva, A.; Bianchi, T.; Catalano, D.; Di Raimondo, M.; Labati, R.D.; Failla, P.; Fiore, D.; Lazzeretti, R.; et al. Privacy-preserving fingerprint authentication. In Proceedings of the 12th ACM Workshop on Multimedia and Security, New York, NY, USA, 9–10 September 2010; pp. 231–240.
6. Jain, A.; Hong, L.; Pankanti, S.; Bolle, R. An identity-authentication system using fingerprints. *Proc. IEEE* **1997**, *85*, 1365–1388. [\[CrossRef\]](#)
7. Wahab, A.; Chin, S.H.; Tan, E.C. Novel approach to automated fingerprint recognition. *IEE Proc. Vis. Image Signal Process.* **1998**, *145*, 160–166. [\[CrossRef\]](#)
8. Bashir, K.; Xiang, T.; Gong, S. Gait recognition without subject cooperation. *Pattern Recognit. Lett.* **2010**, *31*, 2052–2060. [\[CrossRef\]](#)
9. Han, J.; Bhanu, B. Individual recognition using gait enduergy image. *IEEE Trans. Pattern Anal. Mach. Intell.* **2005**, *28*, 316–322. [\[CrossRef\]](#)
10. Wang, L.; Tan, T.; Hu, W.; Ning, H. Automatic gait recognition based on statistical shape analysis. *IEEE Trans. Image Process.* **2003**, *12*, 1120–1131. [\[CrossRef\]](#) [\[PubMed\]](#)
11. Su, K.; Yang, G.; Wu, B.; Yang, L.; Li, D.; Su, P.; Yin, Y. Human identification using finger vein and ECG signals. *Neurocomputing* **2019**, *332*, 111–118. [\[CrossRef\]](#)
12. Meenakshi, V.S.; Padmavathi, G. Security analysis of password hardened multimodal biometric fuzzy vault with combined feature points extracted from fingerprint, iris and retina for high security applications. *Procedia Comput. Sci.* **2010**, *2*, 195–206. [\[CrossRef\]](#)
13. Bronstein, A.M.; Bronstein, M.M.; Kimmel, R. Three-dimensional face recognition. *Int. J. Comput. Vis.* **2005**, *64*, 5–30. [\[CrossRef\]](#)
14. Gu, J.; Zhou, J.; Yang, C. Fingerprint recognition by combining global structure and local cues. *IEEE Trans. Image Process.* **2006**, *15*, 1952–1964. [\[PubMed\]](#)
15. Haq, E.U.; Xu, H.; Khattak, M.I. Face recognition by SVM using local binary patterns. In Proceedings of the 14th Web Information Systems & Applications Conference IEEE, Liuzhou, China, 11–12 November 2017.
16. Kasban, H. Fingerprints verification based on their spectrum. *Neurocomputing* **2016**, *171*, 910–920. [\[CrossRef\]](#)
17. Medina-Pérez, M.A.; Moreno, A.M.; Ballester, M.; Ángel, F.; García-Borroto, M.; Loyola-González, O.; Altamirano-Robles, L. Latent fingerprint identification using deformable minutiae clustering. *Neurocomputing* **2016**, *175*, 851–865. [\[CrossRef\]](#)

18. Nefian, A.V.; Hayes, M.H. An embedded HMM-based approach for face detection and recognition. In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, Phoenix, AZ, USA, 15–19 March 1999; pp. 3553–3556.
19. Zhao, C.; Miao, D. Two-dimensional color uncorrelated principal component analysis for feature extraction with application to face recognition. In Proceedings of the Chinese Conference on Biometric Recognition, Jinan, China, 16–17 November 2013; pp. 138–145.
20. Zhong, F.; Zhang, J. Face recognition with enhanced local directional patterns. *Neurocomputing* **2013**, *119*, 375–384. [[CrossRef](#)]
21. Zhu, L.; Zhang, S. Multimodal biometric identification system based on finger geometry, knuckle print and palm print. *Pattern Recognit. Lett.* **2010**, *31*, 1641–1649. [[CrossRef](#)]
22. Ahmad, M.I.; Woo, W.L.; Dlay, S. Non-stationary feature fusion of face and palmprint multimodal biometrics. *Neurocomputing* **2016**, *177*, 49–61. [[CrossRef](#)]
23. Sun, Q.-S.; Zeng, S.-G.; Liu, Y.; Heng, P.-A.; Xia, D.-S. A new method of feature fusion and its application in image recognition. *Pattern Recognit.* **2005**, *38*, 2437–2448. [[CrossRef](#)]
24. Shan, C.; Gong, S.; McOwan, P.W. Fusing gait and face cues for human gender recognition. *Neurocomputing* **2008**, *71*, 1931–1938. [[CrossRef](#)]
25. Ammour, B.; Bouden, T.; Boubchir, L. Face–iris multi-modal biometric system using multi-resolution Log-Gabor filter with spectral regression kernel discriminant analysis. *IET Biom.* **2018**, *7*, 482–489. [[CrossRef](#)]
26. Khan, M.K.; Zhang, J. Multimodal face and fingerprint biometrics authentication on space-limited tokens. *Neurocomputing* **2008**, *71*, 3026–3031. [[CrossRef](#)]
27. Xiong, Q.; Zhang, X.; Xu, X.; He, S. A Modified Chaotic Binary Particle Swarm Optimization Scheme and Its Application in Face-Iris Multimodal Biometric Identification. *Electronics* **2021**, *10*, 217. [[CrossRef](#)]
28. Frischholz, R.W.; Ulrich, D. BioID: A multimodal biometric identification system. *Computer* **2000**, *33*, 64–68. [[CrossRef](#)]
29. Conti, V.; Militello, C.; Sorbello, F.; Vitabile, S. A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems. *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.* **2010**, *40*, 384–395. [[CrossRef](#)]
30. Soleymani, S.; Dabouei, A.; Kazemi, H.; Dawson, J.; Nasrabadi, N.M. Multi-Level Feature Abstraction from Convolutional Neural Networks for Multimodal Biometric Identification. In Proceedings of the 2018 24th International Conference on Pattern Recognition (ICPR), Beijing, China, 20–24 August 2018; pp. 3469–3476.
31. Aghajari, Z.H.; Teshnehlab, M.; Motlagh, M.R.J. A novel chaotic hetero-associative memory. *Neurocomputing* **2015**, *167*, 352–358. [[CrossRef](#)]
32. Han, Q.; Wu, Z.; Deng, S.; Qiao, Z.; Huang, J.; Zhou, J.; Liu, J. Research on Face Recognition Method by Autoassociative Memory Based on RNNs. *Complexity* **2018**, *2018*, 8524825. [[CrossRef](#)]
33. Hamada, Y.M. Liapunov’s stability on autonomous nuclear reactor dynamical systems. *Prog. Nucl. Energy* **2014**, *73*, 11–20. [[CrossRef](#)]
34. Han, Q.; Liao, X.; Huang, T.; Peng, J.; Li, C.; Huang, H. Analysis and design of associative memories based on stability of cellular neural networks. *Neurocomputing* **2012**, *97*, 192–200. [[CrossRef](#)]