Machine Learning and Intelligent Systems
J.-L. Kim (Ed.)

doi:10.3233/FAIA241214

Research on Traceable Handwritten Signature Anti-Counterfeiting and Verification System

Jiahong YE [a] and Feiyue YE [b] [1]

a School of Data Science, The Chinese University of Hong Kong, Shenzhen, China

b School of Computer Engineering, Jiangsu University of technology, China

Abstract: Addressing the anti-counterfeiting and verification issues of handwritten signatures, a traceable offline handwritten signature anti-counterfeiting and verification system is proposed. The system consists of four parts: a front-end mobile terminal application system, a database storage system, a backend management system, and a portable dynamic encoding stamp device. The system can achieve traceability of signatures, thereby more effectively preventing counterfeit signatures. The front-end mobile terminal application system can generate a unique two-dimensional code based on the relevant information of the signature file and send it to the database system for storage, while also sending it to the portable dynamic encoding stamp device. The portable dynamic encoding stamp device can receive the dynamic two-dimensional code from the front-end mobile terminal application system and produce a two-dimensional code imprint. The database system can store information such as signature file details, corresponding QR codes, and signature photos, which can be used for traceability queries and verification. The proposed system utilizes the SHA algorithm to generate unique codes and can generate corresponding QR code prints on a portable dynamic encoding device. When signing, a QR code seal is affixed, and during signature verification, the QR code on the signature file can be compared with the information in the database to verify the authenticity of the signature. When needed, signature photos stored in the database can also be used for further verification through machine learning. Compared with traditional signature verification methods, this method has better effectiveness.

Keywords: Offline signature, traceability, handwritten signature, signature verification, machine learning.

1. Introduction

Handwritten signatures, as a form of personal identity verification, have widespread applications in many fields such as contract signing, bank transactions, and legal documents. With the development of digital technology, how to accurately and

[1] Corresponding Author, School of Computer Engineering, Jiangsu University of technology, 1801 Zhongwu Rd., Changzhou, Jiangsu, 213001 China; E-mail:yfy@jsut.edu.cn.

efficiently verify the authenticity and consistency of handwritten signatures has become an important research topic. In recent years, handwritten signature verification technology has received widespread attention and in-depth research, with the methods and techniques involved becoming increasingly rich and diverse. Traditional handwritten signature verification methods mainly rely on visual features of the signature, such as penmanship, stroke order, and shape. However, these methods are often affected by various factors such as writing style, paper quality, and environmental conditions, resulting in limited verification accuracy. To improve verification accuracy, researchers have begun to explore the use of machine learning and deep learning technologies for handwritten signature verification. These methods can automatically extract features from a large amount of signature data and use complex models for classification and recognition, thereby greatly improving the accuracy and robustness of verification. In addition to methods based on visual features, some researchers have attempted to use other types of features for handwritten signature verification, such as sound and motion sensor data. These methods provide new ideas and directions for handwritten signature verification but also bring new challenges and problems. For example, how to effectively extract useful features from complex sound signals, how to handle differences between different writers, etc. Moreover, with the popularization of mobile devices and wearable devices, some researchers have begun to explore the possibility of performing handwritten signature verification on these devices. These devices are usually equipped with various sensors that can capture users' hand movements and physiological information in real-time, providing a rich data source for handwritten signature verification. However, at the same time, achieving efficient and accurate handwritten signature verification on these devices is also an urgent problem that needs to be solved. The aforementioned methods have issues related to the accuracy and efficiency of verification. Therefore, it is crucial to find a method that can ensure the correctness of signatures. This paper will study a signature verification system that combines database technology with dynamically encoded seals and signatures at the front end. Using this system, a dynamically encoded seal is applied while signing, and the signature information is saved in the database, enabling traceability of the signature. This has positive implications for the anti-counterfeiting of signatures.

2. Relevant Research

Signature verification, a subfield of behavioral biometrics, primarily focuses on identity verification through the analysis of individual signature characteristics. These characteristics encompass speed, frequency, morphology, and spatial geometric features of the signature, all of which can be utilized to differentiate between genuine and forged signatures. As technology advances, researchers are increasingly exploring methods to enhance the accuracy and stability of the signature verification system. In 2014, a novel offline handwritten signature recognition and verification system was proposed [1]. This system recognizes and verifies the signature by calculating the fractal dimension. Experimental results demonstrated that the system achieved a recognition rate of 95% and a verification rate of 83% on the large database "FUMPHSDB". Furthermore, a personal recognition process for handwritten signature owners based on motion detection

and QR codes was proposed [2]. The system employs motion detection technology to identify the actual hand movements during the signature process, thereby preventing others from imitating or copying the signature. By integrating QR code technology, a unique code is created for each signature, which is stored alongside the signature and used to verify its authenticity. When the user attempts to authenticate, the system simultaneously requires the user to provide a handwritten signature and the corresponding QR code. If the system detects that the user's hand movements match the stored QR code, and the signature appears genuine (i.e., without obvious signs of imitation), then the authentication is allowed to succeed. In 2015, a paper proposed a new offline handwritten signature verification method that combines fine-grained intensity features and global geometric features [3]. This pioneering system leveraged variations in acoustic signals to facilitate signature verification. Distinct from prior acoustic sensing systems, ASSV employed an innovative chord-based approach to estimate phase-related alterations induced by minute movements. In 2020, a comprehensive analysis of existing signature verification techniques led to the proposal of an identity authentication system grounded in handwriting features [4]. Concurrently, some studies identified the sounds produced by paper and pen friction as potential biodata for handwritten signature verification [5]. These sounds were captured using two distinct mobile phone models. To broaden the scope of the study, data collection encompassed participants across various age groups, utilizing diverse pens, papers, and mobile phones. In 2021, a novel model was introduced for verifying dynamic handwritten signatures [6], employing neutral logic rules and genetic neutral logic rule models. In the same year, a deep signature verification model was proposed [7], comprising three fundamental stages: deep feature generation via transfer learning, iterative minimum redundancy maximum relevance (IMRMR) feature selection, and classification. Furthermore, A signature anti-counterfeiting method and the basic framework of the anti-counterfeiting system are proposed [8]. In 2022, a signature verification protocol tailored for touchscreen devices was presented [9]. Diverging from traditional geometric feature-based methods, this approach extracts the primary frequency components of the speed signal during the signing process and stores them for comparison via barcodes. To realize this objective, a specialized interface was designed to monitor the signing process and extract displacement data. Subsequently, the speed signal undergoes interpolation and spectral analysis through continuous wavelet transform (CWT), yielding a 4-scale spectrogram, which is then classified using a support vector machine (SVM). Experimental results indicate that this method yields competitive outcomes across multiple datasets. In 2024, in order to investigate the impact of environmental or internal pressures on individual signature registration, as well as their subsequent effects on the performance of signature verification systems. The researchers aim to use muscle synergy as a biological feature to study the efficacy of these systems when applied to populations under stress. To achieve this goal, they recorded electromyographic (EMG) signals of hand and arm muscles and used non negative matrix factorization (NMF) method to extract muscle synergy effects from the preprocessed EMG signals. Subsequently, the extracted synergistic effects were classified into real and fake categories using a support vector machine (SVM) classifier [10].

Over the past decade, numerous researchers have concentrated on the issue of handwritten signature verification, adopting a variety of methods and techniques to

enhance the accuracy of signature verification. They all underscored the significance of feature extraction, employing various techniques for this purpose. However, their approaches to addressing the problem varied. Some primarily focused on integrating fine-grained intensity features with global geometric features, while others sought to improve accuracy by expanding the collection of user handwriting information and perfecting the handwriting sample library. In summary, these papers offer valuable insights and methodologies for research on handwritten signature verification.

3. A Traceable Handwritten Signature Verification System

3.1 Basic Architecture

As shown in Figure 1, the handwritten signature verification system mainly consists of a front-end mobile terminal application system, a database storage system, a back-end management system, and a dynamic encoding seal device. The front-end mobile terminal application system can input signature information, including the file name of the signature, time, location, etc., and generate an encryption code based on this information. This code is sent to the dynamic encoding seal device via the communication system and also sent to the database storage system, where it records the encryption code along with corresponding file names, locations, times, etc. The database storage system can save the code information and corresponding details, including signature photos. The back-end management system can query signature information, including corresponding encryption codes and signature photos. Additionally, as needed, it can analyze the signature photos to verify the authenticity of the signatures. The dynamic encoding seal can receive the code information from the mobile terminal to generate an encoded seal body and send relevant printing information to the database storage system to save the corresponding signature and printing information.

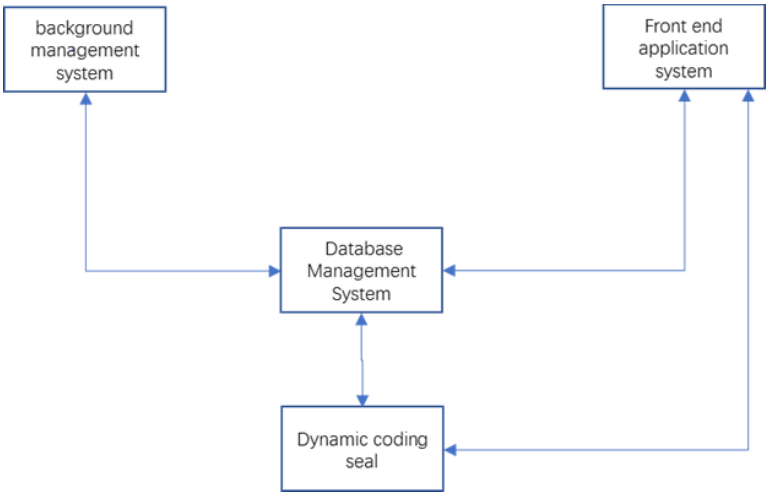

Figure 1 Basic Architecture of the System

As shown in Figure 2, it is an example image with a dynamic QR code signature implemented by this system. The system generates a different password for the signature of different file contents, and according to the corresponding unique password, the corresponding QR code is generated through QR code generation software. This QR code and its related information are recorded in the database system for later verification.

Figure 2 Example of Signature with Dynamic QR Code Seal

3.2 Front-end Application System

The front-end application system includes relevant information for inputting signature data, such as the file name of the signature, time, and location, and generates encrypted codes through an encoding generation program. The front-end application system also has the function of communicating with database management systems and dynamic code seals. The front-end application system can save the name, time, location, and encrypted code of the signature file into the database management system through a communication system, while also querying and verifying related information in the database management system based on permissions. As shown in Figure 3, the dynamic code is generated by applying the SHA to the signature file's name, time, and location, and a corresponding QR code is generated using a QR code generation program. Simultaneously, the QR code and related information are saved into the database system. At this point, the QR code information is sent to the portable dynamic code seal device via communication.

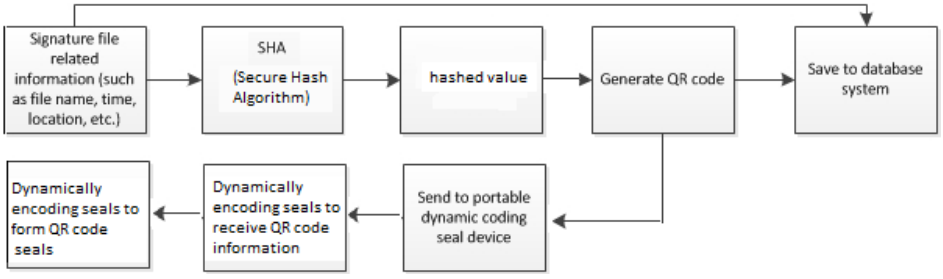

Figure 3 Dynamic encoding generation and transmission of front-end application system

3.3 Backend Management System

The backend management system includes functions such as user management, encryption algorithm updates, data queries, and signature verification. User management functions include user information management, user permission settings, user information queries, etc., and encryption algorithm updates.

3.4 Portable Dynamic Code Stamp Device

The stamping device is a portable dynamic code stamp with wireless communication capabilities, capable of receiving dynamic code information sent from the front-end application system. Based on the received code information, it can form a code imprint under a certain force, becoming a dynamic code stamp. In addition, the stamp device can also signature information to the database management system for storage through wireless communication, as shown in Figure 4.

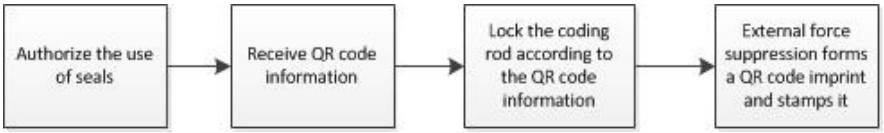

Figure 4: Dynamic Encoding Print Generation and Printing

The basic structure schematic diagram of the portable dynamic encoding seal device is shown in Figure 5.[11]

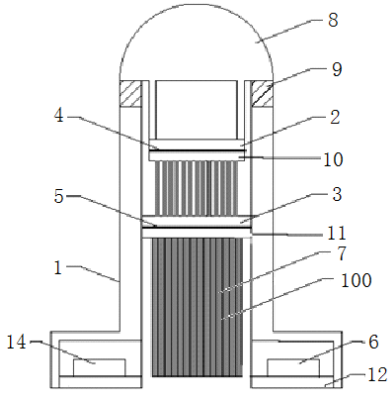

Figure 5 Portable dynamic coding seal device

The portable dynamic coding seal device includes: pressure button 8, elastic component 9, locking systems 4 and 5, guide rail assembly 10, coding rod assembly 100, and fixed frame 3; Activity rack 2, information processing module 14, seal body 12, external shell 1, in addition to power supply, power switch, display screen, etc. The communication

module in the information processing module of the seal device receives the seal opening information, and the encoded information is received through the communication module. The controller in the information processing module controls the switch circuit based on the encoded information, thereby controlling the locking system to lock the encoding rod. Under the joint action of the locking system and the pressure button, the target encoding rod can move downward according to the encoding rules, forming an encoding seal.

The working principle of the portable dynamic coding seal device is as follows: turn on the power switch on the housing, turn on the information processing module in the device, and the identity authentication module starts working. The authentication prompt is displayed on the display screen for operation. The identity authentication module receives the information for authentication. After passing the authentication, the device enters the working state. After receiving the external coding information, the information processing module processes it and controls the corresponding locking device to press the button downwards. Under the action of the locking device, the coding rod group forms the required coding seal body and implements the seal function. At the same time, it sends the print information to the external database. After the stamping is completed, the upper pressure is released. Under the action of the elastic module, the state is restored.

3.5 Signature Verification

The signature verification of this system mainly uses a unique QR code generated by SHA (Secure Hash Algorithm) to verify the relevant information of the signed file, such as file name, signature time, signature location, etc. When necessary, machine learning methods can also be used to assist in the verification of the signed image. The method of using QR code for verification is shown in Figure 6. Firstly, the client can scan the QR code next to the file signature. The client program first queries whether the code exists in the database. If it does not exist, the signature file is fake. If there is a seal QR code, the corresponding signature file information (such as signature time, signature location,

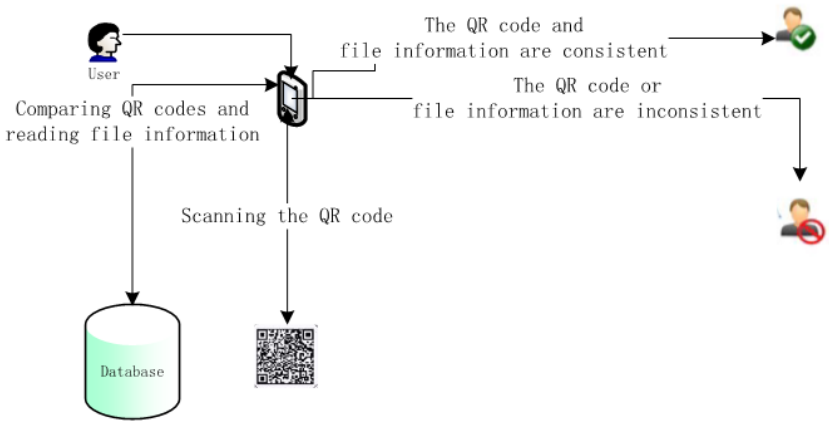

Figure 6 Compare using QR code and file information

file name, etc.) is returned and compared with the signature file in the file. If the signature file information in the database is consistent with the information in the signature file, it

is a true signature. Otherwise, there is a contradiction in the information, Further verification is needed (note: under normal circumstances, that is, while ensuring the security of seal use, communication security, and database security, this situation should not occur, because the QR code generated by using SHA for signature file information is unique, and the information saved in the database is also unique, so there should be no contradiction). If there is an information conflict during the QR code verification process, the signature image can be further used for verification. The verification process is as follows: the client takes a photo of the signature in the file and compares it with the signature image in the corresponding QR code record in the database through machine learning methods. If the comparison result meets the consistency threshold requirement, the signature is true; Otherwise, there will be doubts about the required signature.

4. Conclusion

This paper presents a novel method for anti-counterfeiting and verification of handwritten signatures, based on an analysis of existing signature anti-counterfeiting and verification techniques. The proposed approach integrates signatures with dynamic QR codes, offering superior traceability and enhanced authenticity assurance compared to current methods. This development has significant implications for the smooth operation of business activities and social stability.

References

[1] R Zouari, R Mokni，M Kherallah. Identification and verification system of offline handwritten signature using fractal approach. 2014 International Conference on Image Processing Applications and Systems, 2014 November 05-07; Sfax, Tunisia. pp1-4.

[2] P Subpratatsavee, P Pudtuan, J Charoensuk, T Sondee, T Vejchasetthanon. The Authentication of Handwriting Signature by Using Motion Detection and QR Code. 2014 International Conference on Information Science & Applications (ICISA),2014, May, pp1-4.

[3] DingFeng Wang, Dong Zhang, Qian Zhao. ASSV: Handwritten Signature Verification Using Acoustic Signals. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.2019 September; 3(3), Article 80: 1-22.

[4] AV Beresneva, AV Epishkina. Approaches to online handwritten signature verification. Information Technology Security,2020,27(2):78-85.

[5] MS Sadak, N Kahraman, U Uludag. Handwritten Signature Verification System Using Sound as a Feature. 43rd International Conference on Telecommunications and Signal Processing (TSP), 2020,pp365-368.

[6] Amr Hefny, Aboul Ella Hassanien and Sameh H. Basha. Neutrosophic Rule-Based Identity Verification System Based on Handwritten Dynamic Signature Analysis, Computers. Materials & Continua, 2021, 69(2):2367-2385.

[7] O Alpar. Signature barcodes for online verification. Pattern Recognition，2022.124（10826）:1-16.

[8] Jiahong Ye, Feiyue Ye. Signature anti-counterfeiting method and signature anti-counterfeiting system[p], CN202011062007.8. 2021-08-27.

[9] T Tuncer, E Aydemir, F Ozyurt, S Dogan. A deep feature warehouse and iterative MRMR based handwritten signature verification method. Multimedia Tools and Applications, 2021, November; 81:3899–3913.

[10] Arsalan Asemi, K. Maghooli, H. Azadeh. The effect of individual stress on the signature verification system using muscle synergy. Biomedical Signal Processing and Control, 2024,88(105040):1-9.

[11] Jiahong Ye, Feiyue Ye, Yuxi Shi. Dynamic coding anti-counterfeiting seal device[p]. CN202211655912.3. 2023-03-31.