processes

MDPI

Article

Dynamic Signature Verification Technique for the Online and Offline Representation of Electronic Signatures in Biometric Systems

Juanjuan Huang [1,*], Yuhang Xue [2] and Linhui Liu [2]

[1] Department of Criminal Science, Hunan Police Academy, Changsha 410138, China
[2] Student Brigade, Department of Criminal Science and Technology, Hunan Police Academy, Changsha 410138, China
* Correspondence: huangjj@hnpa.edu.cn

Abstract: Biometric systems input physical or personal human characteristics for identification, authentication, and security purposes. With the advancement in communication and intelligent security systems, biometrics are programmed to validate electronic signatures (E-signatures) for online and offline authentication. This article introduces a dynamic signature verification technique (DSVT) using mutual compliance (MC) between the security system and the biometric device. The security system is responsible for online and offline signature approval using personal inputs from humans. This personal verification is related to the stored online/offline signatures using certificates provided for authentication. The certificate-based authentication is valid within a session for online representation. Contrarily, this authentication is valid for persons under offline conditions. In this mode of segregation, application-level authentication verification is performed. A conventional tree classifier for dynamic signature verification is used for differentiating online and offline signatures. Moreover, the security metrics—such as signing bit, key, and size—are verified for both modes using classifier learning. For the segregated mode, the validation of the above is required to be unanimous to accelerate the dynamicity. The proposed technique's performance is analyzed using the authentication success rate, verification failing ratio, verification time, and complexity.

Keywords: biometric system; classifier learning; E-signatures; signature verification

Citation: Huang, J.; Xue, Y.; Liu, L. Dynamic Signature Verification Technique for the Online and Offline Representation of Electronic Signatures in Biometric Systems. *Processes* **2023**, *11*, 190. https://doi.org/10.3390/pr11010190

Academic Editor: Wen-Jer Chang

Received: 31 October 2022
Revised: 28 December 2022
Accepted: 28 December 2022
Published: 6 January 2023

1. Introduction

A biometric signature is a pattern of electronic documents that are stored in a database for biometric systems. Electronic documents are mostly based on handwritten signatures using computer screens and other electronic devices. Biometric signatures are widely used in systems for authentication and authorization processes [1]. Biometric signature verification (BSV) is a crucial and important task to perform in biometric systems and applications. Biometric signatures provide necessary measures, features, and patterns for authentication that reduce the error ratio from accessing users' data [2]. Digital signature pads are used in biometric systems to obtain accurate information about signatures. Digital pads detect optimal data that are required for BSV, which enhances the accuracy of the verification process [3]. The behavioral biometric technique is also used for BSV that detects the behavior of users' signatures. Digital pads provide necessary information for verification techniques that provide features and details of signatures. Users' behaviors contain accurate data related to signatures that achieve high accuracy in the authentication process [4,5].

Biometric systems are most widely used in various fields to reduce paperwork and improve security levels. Digital signatures are used in both online and offline biometric systems. Digital signature verification is a complicated task to perform in biometric systems [6]. Various methods and techniques are used for the biometric signature verification (BSV) process. Field-programmable gate arrays (FPGAs) are used in online digital signature verification. A recognition algorithm is used in FPGAs to detect necessary patterns

and details of digital signatures [7]. FPGAs capture the exact moves, positions, noises, and patterns of signatures that reduce latency levels in signature verification. The vector floating-point unit (VFPU) method is also used in BSV to identify floating-point values of signatures [8]. VFPUs are calculated based on a benchmark database that contains exact values of signatures. The hidden Markov model (HHM) is used for the digital BSV process. The HHM is mostly used for offline digital verification in biometric systems [9]. A feature extraction method is used in HHM that extracts important features from the biometric database, which provide relevant information for BSV. The HHM maximizes the security and feasibility ratio of the biometric system by providing proper policies to users [10].

Dynamic biometric signature verification is widely used for verifying the exact identities of users' signatures. Dynamic biometric signature verification is mostly implemented during the authentication process [11], which requires accurate information. A global and regional information-based hybrid algorithm is used for dynamic signature verification. Hybrid algorithms verify the variations and patterns of digital signatures that are stored in the database [12]. Both global and regional information provide necessary data for verification that reduces latency levels in identification. A convolutional neural network (CNN)-based technique is also used in dynamic signature verification [13]. CNNs use feature extraction method that extracts important features and details of signatures for the authentication process. CNNs reduce the overall error and time consumption levels in authentication, enhancing the performance and efficiency of biometric systems [14]. The artificial neural network (ANN) algorithm is commonly used for dynamic signature verification. The pixel-matching technique (PMT) is used in ANNs to detect the exact matching pixels of the signature for the authentication process. The PMT achieves high accuracy in detection and improves the effectiveness ratio of authentication in biometric systems and applications [15].

However, the existing systems fail to predict the human characteristics with the minimum matching failure rate. In addition, the biometric validation requires additional effort to minimize the computational complexity. This research issue can be overcome by applying the dynamic signature verification technique (DSVT) using mutual compliance (MC) between the security system and the biometric device. The algorithm uses the authentication procedure and signature verification process to improve the overall authentication. In addition, the mutual compliance process reduces the matching failure rate. The discussed system's efficiency is evaluated using the experimental results and discussion.

The rest of this paper is organized as follows: Section 2 discusses the various researchers' opinions about the biometric authentication process. Section 3 analyzes the working process of DSVT- and MC-based verification and authentication processes. Section 4 describes the efficiency of the introduced DSVT- and MC-based verification process. The conclusions are summarized in Section 5.

2. Related Works

Tolosana et al. [16] introduced a new time-aligned recurrent neural network (TA-RNN) approach for the online signature verification process. The proposed method is a deep learning approach that identifies features of biometric signatures from the database. An RNN is used here to train the data that are required for signature verification, which reduces latency in identification. When compared with other approaches, the proposed TA-RNN approach improves the performance and efficiency of signature verification. However, the system takes a long time to verify the signature.

Bassit et al. [17] developed a biometric verification protocol based on a homomorphically encrypted log-likelihood ratio (HELR) classifier for biometric systems. The HELR classifier is mainly used here to detect features and patterns of biometric signatures. The HELR classifier predicts the exact information about signatures for the verification process. HELR improves the security ratio of the signatures. The proposed protocol achieves high accuracy in verification and enhances the feasibility and effectiveness of biometric systems. The system consumes more computational effort while deriving the biometric pattern.

Ponce-Hernandez et al. [18] introduced a fixed-length template-based fuzzy vault (FV) scheme for dynamic signature verification (DSV). The proposed FV scheme is mostly used in biometric template protection (BTP) that requires accurate information for verification. FVs extract both global and important factors of signatures that reduce the energy consumption levels in computation. Fixed-length templates increase the security and safety of biometric signatures from attackers. The proposed FV scheme improves the performance, robustness, and reliability of DSV. The biometric template protection consumes more time, and complex patterns are difficult to manage.

Yang et al. [19] proposed a cancellable fingerprint authentication system based on linear convolution for biometric systems. Linear convolutional functions and vectors are used here that provide relevant information for authentication. The feature extraction technique is used to extract the necessary patterns and features of signatures. The proposed system maximizes accuracy and efficiency in verification and recognition, enhancing security in the authentication process.

Parcham et al. [20] introduced a convolutional neural network (CNN)- and capsule neural network (CapsNet)-based offline signature verification model. The CNN is mainly used to identify important features, patterns, and factors of signatures that provide relevant data to the signature verification model. CapsNet is used to reduce the complexity level in computation. The experimental results showed that the proposed model maximizes the accuracy level in signature verification, improving the performance of biometric systems.

Okawa et al. [21] introduced a single-template matching method based on local stability-weighted dynamic time warping (LS-DTW) for online signature verification. LS-DTW is used here to obtain optimal warping templates for verification that reduce the complexity level in computation. The templates are trained and produced to the matching method that accurately detects the signatures of users. When compared with other methods, the proposed method achieves high accuracy in verification, improving the performance and mobility of the systems.

Dhieb et al. [22] designed a score-level fusion-based signature verification method for biometric systems. Machine learning (ML) algorithms are used here to enhance the effectiveness of the verification process. Deep bidirectional long short-term memory (Deep BiLSTM) is used here to extract both static and dynamic features from signatures. The score-level fusion approach is mainly used here to obtain optimal information for verification. The proposed verification method improves the efficiency and reliability of online signature verification in biometric systems. The score-level fusion fails to manage the complex patterns.

Naz et al. [23] developed a new signature verification system based on a fine-tuned transfer learning approach. The proposed system is mostly used for offline signature verification to investigate the features and patterns of users' signatures. The fine-tuned transfer learning approach is used here to identify offline images of signatures that produce optimal data for verification. The proposed system maximizes the stability, mobility, and feasibility levels of biometric systems.

Yang et al. [24] introduced an effective and privacy-preserving cloud-based biometric identification scheme (MASK) for biometric systems. MASK is mostly used to understand and identify user requests that occur during communication services. MASK reduces the overall time and energy consumption levels in verification. An M-tree structure is used here to detect necessary data for signature verification. When compared with other methods, the proposed scheme enhances the performance of signature verification in biometric systems.

Houtinezhad et al. [25] designed a bag of features in the candidate point (BoF-CP) model for offline signature verification in biometric systems. Standard information and datasets are used here that provide relevant data for verification. Homogeneous feature vectors are detected based on certain images and templates that reduce the complexity ratio in computation. The proposed BoF-CP model achieves high accuracy in verification, improving the sensitivity and reliability of biometric systems.

Roy et al. [26] introduced a graph neural network (GNN)-based offline signature verification model. Target nodes in graphs are detected based on features that provide

necessary information for prediction, detection, and recognition processes. Test signature samples are trained based on target nodes that reduce latency in the identification process. The proposed GNN-based model improves verification accuracy to provide proper services to users.

Tan et al. [27] proposed a new gene expression programming (GEP)-based online signature verification method for biometric systems. A backpropagation neural network classifier is used here that classifies vectors and functions relevant to biometric signatures. The feature extraction technique is also used here to extract important features and patterns of signatures. The proposed method enhances the overall performance and efficiency levels of biometric systems by improving accuracy in signature verification.

Saleem et al. [28] introduced an online signature verification method based on down-sampling and signer-dependent sampling frequency. The sampling frequency range is a measure based on certain vectors and functions. Sampling frequency provides relevant data for signature verification, reducing the time consumption level in computation. The experimental results showed that the proposed method achieves high accuracy in verification and prediction, improving the effectiveness ratio of biometric systems.

Motivation

According to various researchers' opinions, the biometric verification and user authentication process can be managed by several approaches. These methods are able to manage the system's reliability, robustness, and effectiveness; however, the existing systems require high computational complexity when handling complex patterns. These difficulties can be overcome by applying dynamic signature verification in biometric systems. This process uses mutual compliance (MC) to improve the overall verification and authentication efficiency.

3. Proposed Technique

In this section, we first introduce the challenges and design goals of our dynamic signature verification system. This article illustrates a novel approach to computing E-signatures for online and offline authentication in biometric systems. The biometric systems and remote devices are mainly used for human identification, authentication, and security purposes, validating electronic signatures for online and offline authentication related to the total stored biometric systems. The biometric systems are classified as online or offline signature approval using a tree classifier. This E-signature approval is processed using observation of personal inputs from humans. This personal verification of humans is analyzed based on stored online/offline signatures using certificates and a person's authentication within mutual sessions. E-signature-based online and offline authentication is vulnerable in terms of validating accurate electronic signatures where attackers cannot observe and replicate the particular user information for authentication. The dynamic signature verification computation in biometric systems provides digital certificates for making decisions to improve authentication in data communication. The authentication success rates for dynamic signature verification in biometric systems were analyzed while the differentiation of online and offline signature validation was performed. In Figure 1, the proposed DSVT-MC is illustrated.

The proposed technique was successfully applied in both online and offline representation with well-known dynamic signature verification to validate the number of physical and personal human characteristics identified for security purposes. Dynamic signature verification in biometric systems and remote devices improves security due to application support with maximum and minimum authentication provided along with security measures. The challenge in identifying verification failures based on the signing bit, size, and key is that the available security metrics satisfy less authentication verification at different time intervals. This time session can be computed through a learning process for preventing verification failures and complexity. Therefore, electronic signature verification for online and offline authentication in the biometric system ensures reduced verification time in a biometric system. The mutual session for both the online and offline signature approval is

an important consideration in this proposed technique. The DSVT using MC between the security system and the biometric device is performed for online and offline representation by providing minimum or maximum security systems for digital signature verification. In this proposal, verification failures and complexity are administrable for both online and offline signature approval in the mutual sessions at the time of information exchange through high-risk intelligent security systems. To avoid this risk factor, this article is based on dynamic signature verification and digital certificates.

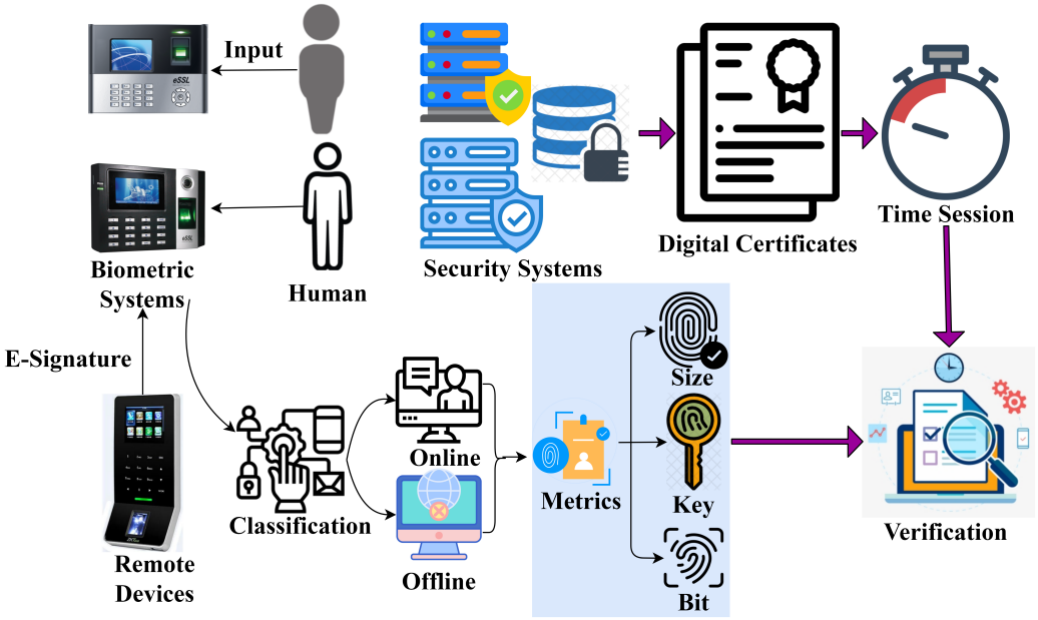

Figure 1. DSVT-MC illustration.

The proposed technique includes different security systems and digital certificates that serve as inputs to the mutual sessions in biometric systems. The proposed technique is used for digital signature verification using mutual sessions between the security systems and remote devices. In this proposal, a high authentication success rate is achieved with the help of biometric systems and provides certificates for the E-signature for online representation to easily satisfy verification, minimum failures, and complexity in biometric systems. Furthermore, the tree classifier is used to differentiate the online and offline signatures in the biometric systems and remote devices based on verification time to improve the security systems. This is a better way of illustrating how the results are determined based on our human physical and personal observations and required by application-level authentication and certificate-based authentication in our case study.

3.1. Dynamic Signature Verification

When the dynamic signature verification is computed for both online and offline signature, it has no limit for authentication satisfied by the human, making it possible to change the communication techniques and intelligent security systems for better security in biometric systems. We perform the dynamic signature verification equation for the particular humans with E-signatures in a biometric system along with the security systems (S). The security system is responsible for online and offline signatures based on the user information at different input observation intervals i for verification and authentication time. Attackers may attempt to steal legitimate users' E-signature patterns to observe their identification and information to gain benefits. For example, attackers can copy some knowledge of the human E-signature and sign in to unauthorized biometric systems or modify the available user's information through E-signature fraud. It is possible to identify this attacker through the dynamic signature verification technique, as follows:

$$H_iS = B_s + R_D - ON_{SS} - OFF_{SS} - A_{verify} - MCsin(\Delta) \quad (1)$$

In Equation (1), $H_i \rightarrow$ personal input from humans, $S \rightarrow$ security systems, $A_{verify} \rightarrow$ authentication verification for both online and offline verification, $B_s \rightarrow$ biometric systems, $R_D \rightarrow$ remote devices, $ON_A \rightarrow$ online signature authentication, $OFF_A \rightarrow$ offline signature authentication, $MC \rightarrow$ mutual compliance, and $\Delta \rightarrow$ mutual session authentication verification. Based on the instances, the individual user information authentication verification can be classified into two segments, namely, online signature and offline signature, which are separately processed every time. In our approach, we differentiate online and offline signature approval that follows the user's digital signing behavior to improve the accuracy of dynamic signature verification and reduce adversarial E-signature forging activities in biometric systems. To identify the online and offline signatures of a user's authentication information, we compare the current E-signature from the user with stored online/offline signatures to prevent forging activities. The digital signature verification is estimated as follows:

$$ON_{SV} = mON_{SS} \quad (2)$$

$$OFF_{SV} = mOFF_{SS} \quad (3)$$

$$A_{verify} = \frac{1}{2}D^C E_{sign} DS_{verify} VF^2 \quad (4)$$

In Equations (2)–(4), $m \rightarrow$ security metrics for modes, $ON_{SS} \rightarrow$ online signature approval, $OFF_{SS} \rightarrow$ offline signature approval, $D^C \rightarrow$ digital certificates provided for authentication, $E_{sign} \rightarrow$ electronic signature for both modes, $DS_{verify} \rightarrow$ digital signature verification, and $VF \rightarrow$ verification failing ratio. With the E-signature in the remote devices for the biometric systems, we can validate both online and offline signature verification assuming that the application-level authentication is performed:

$$ON_{SS} = \frac{1}{C_A + P_A}\left[-A_{verify}ON_S/OFF_S - \alpha\Delta T - MCXsin(\Delta) + MCC_Acos(\Delta)\right] \quad (5)$$

$$OFF_{SS} = \frac{1}{C_A + P_A}\left[A_{verify}ON_S/OFF_S + \alpha\Delta T + MCXsin(\Delta) + MCP_Acos(\Delta)\right] \quad (6)$$

In Equations (5) and (6), $C_A \rightarrow$ certificate-based authentication within a time session that is valid for online representation, $P_A \rightarrow$ this authentication for specific personal verification is valid for offline representation, $T \rightarrow$ authentication verification time, and $\alpha \rightarrow$ authentication success rate. Based on Equations (5) and (6), the first E-signature of the user is observed by the remote devices for all $ON_{SS} + OFF_{SS}$ responsible for complete online and offline signing of individual users at any time interval on $VF \times T$. Here, VF is used for identifying the verification failure in biometric systems. This personal verification of the unique user is performed to reduce the forging activities in the present communication. The signature verification and approval processes are illustrated in Figure 2.

The H_i is sensed by the B_S for online and offline features such that different signatures are used for verification. In the case of stored D^c, the ON_{SV} and OFF_{SV} are used for E_{sign} verification. If the $VF \times T$ interval matches the stored D^c or H_i credentials, then approval is provided. Conversely, if the session failure occurs, then authentication is transferred to the next session $\forall\ ON_{SS} + OFF_{SS}$ (Figure 2). If any changes are identified at the time of signing, the current signature size, bit, and key are compared with the stored online/offline signatures to accurately detect the dynamic signature of that particular user in any T. This instance of digital signature verification follows a high authentication success rate that is represented as follows: The remotely connected E-signature devices in biometric systems are responsible for both online and offline signature verification using generated security metrics such as signing bit, key, and size. The security metrics are generated as follows:

$$B_S = SZ_{ON}Ky_{ON}Bt_{ON} \quad (7)$$

$$= SZ_{OFF}Ky_{OFF}Bt_{OFF} \quad (8)$$

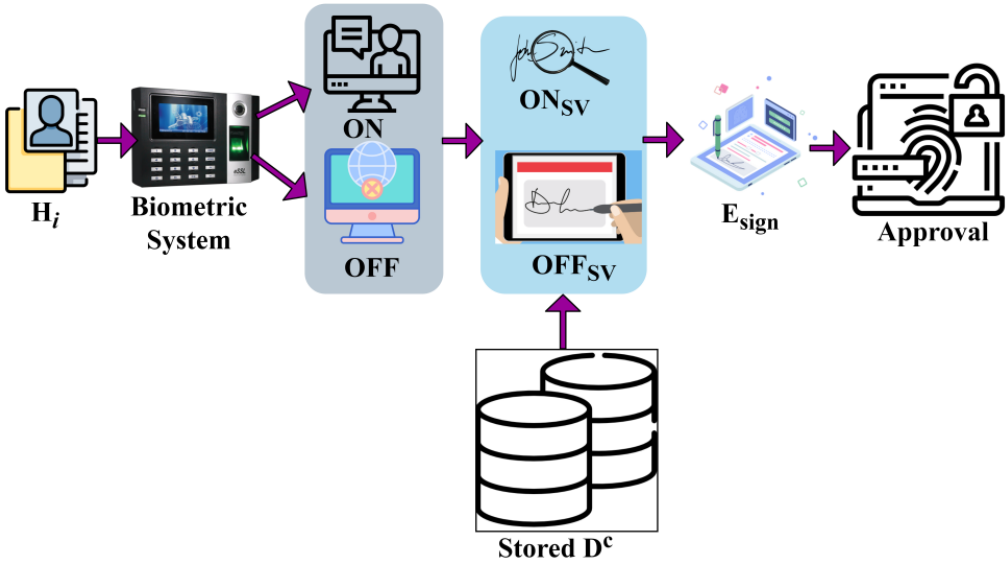

Figure 2. Signature verification and approval.

In Equations (7) and (8), $SZ \rightarrow$ signing size, $Ky \rightarrow$ signing key, and $Bt \rightarrow$ signing bit. The online and offline signature authentication rate is defined as follows: Equations (7) and (8) compute the digital signature verification of individual users' information for failure and complexityless signature verification is detected after performing certificate-based authentication. From the instances, the individual user authentication verification is performed using security metrics. Security metrics can be classified into three features (signing bit, key, and size) observed for all users, because these are all of the unique features identified by the users at the time of digital signing in biometric systems. Equations (7) and (8) are used to validate the signing size (SZ), key (ky), and bit (Bt) for dynamic signature verification of individual users; authentication is computed as follows:

$$SZ = \frac{MS_{ON} - VF}{T} \tag{9}$$

$$Ky = \frac{MS_{OFF} - VF}{T} \tag{10}$$

$$Bt = \frac{MS_{ON}/MS_{OFF} - VF}{T} \tag{11}$$

In Equations (9)–(11), $MS_{ON} \rightarrow$ mutual session timing for online authentication and $MS_{OFF} \rightarrow$ mutual session timing for offline authentication. The mutual session timing for individual user identification and authentication is computed as follows:

$$MS_{ON} = MS_0 - \frac{SZ + Bt}{Ky_t} \tag{12}$$

$$MS_{OFF} = MS_0 - \frac{SZ + Bt}{Ky_t} \tag{13}$$

In Equations (12) and (13), $MS_0 \rightarrow$ unauthorized mutual sessions in biometric systems and $Ky_t \rightarrow$ key verification time. Similarly, the abovementioned adversarial forging activities are addressed, in that biometric systems use dynamic signature verification to reduce the verification failure ratio and complexity.

3.2. Classification through Mutual Service

The classification through mutual service is illustrated in Figure 3.

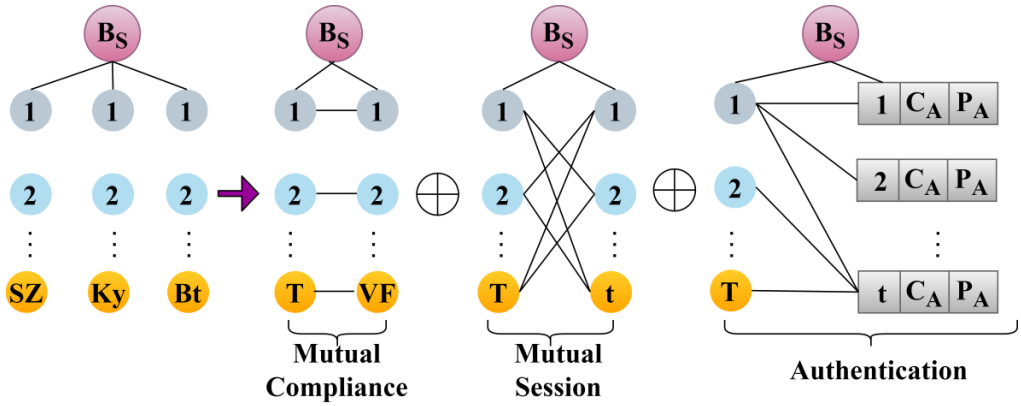

Figure 3. Classification through mutual service.

The security system performs an integrated classification for SZ, Ky, and Bt. The MC, session (T, t), and authentication are precise over VF, t, and (C_A, P_A). In all cases, the MS_{ON} and MS_{OFF} are validated across VF/T provided that multiple sessions are approved. Therefore, the available sessions are used for signing and verifying the signatures in leveraging verification (see Figure 3) if an unauthorized biometric system observing users' information causes verification failures. In this mode, segregation of online and offline signatures is performed to improve the application-level authentication using tree classifiers and security metrics. In this instance, the sequential online and offline signature approval in biometric systems is estimated as follows:

$$ON_{approval} = -MS_{ON} A_{verify} - VF - T \tag{14}$$

$$OFF_{approval} = -MS_{OFF} E_{sign} - VF - T \tag{15}$$

We assume that the E-signature in the biometric system is used to provide a certificate for authentication along with the stored online/offline signatures for personal verification. This verification failure at the time of the digital signing process is prevented by analysis of security metrics for accurate user information authentication at both online and offline signing verification, along with the digital certification at various session times. Based on this, the classification process assists in addressing the forging activities by verifying the remotely connected devices and security metrics for all online/offline signature modes. The classification process is performed to differentiate the online and offline signatures using tree classifier learning. In this proposal, the abovementioned unique features of users' E-signatures are independently analyzed and verified in biometric systems using certificates provided for user information authentication.

$$A_{verify} = \alpha_t T \tag{16}$$

$$P_{verify} = (1 - \alpha_t) T \tag{17}$$

where $A_{verify} \rightarrow$ both modes of authentication verification, $P_{verify} \rightarrow$ both modes of personal verification, and $v\alpha_t \rightarrow$ verification time for individual user information authentication and identification. To accelerate the dynamicity in both online and offline signatures at various verification times, instances for a unique user are analyzed. Similarly, the first human physical and personal information is observed to prevent user authentication failures; therefore,

$$ON_S = A_{verify} + v\alpha_t - VF \tag{18}$$

$$OFF_S = P_{verify} + v\alpha_t - VF \tag{19}$$

Equations (18) and (19) are validated separately for the online and offline signatures at which digital certificates are provided for accurate dynamic signature verification. If the time session for the signing process is computed for both modes and then the verification time is computed, this verification is a considerable factor in biometric systems. Addressing

forging activities in biometric systems at the time of performing E-signatures at T intervals prevents complexity. This is because the changes are identified in the users' information and certificate outputs in verification failure. Here, the verification output for $A_{verify} \neq P_{verify}$ is computed. The information verification through the online signature process is portrayed in Figure 4.

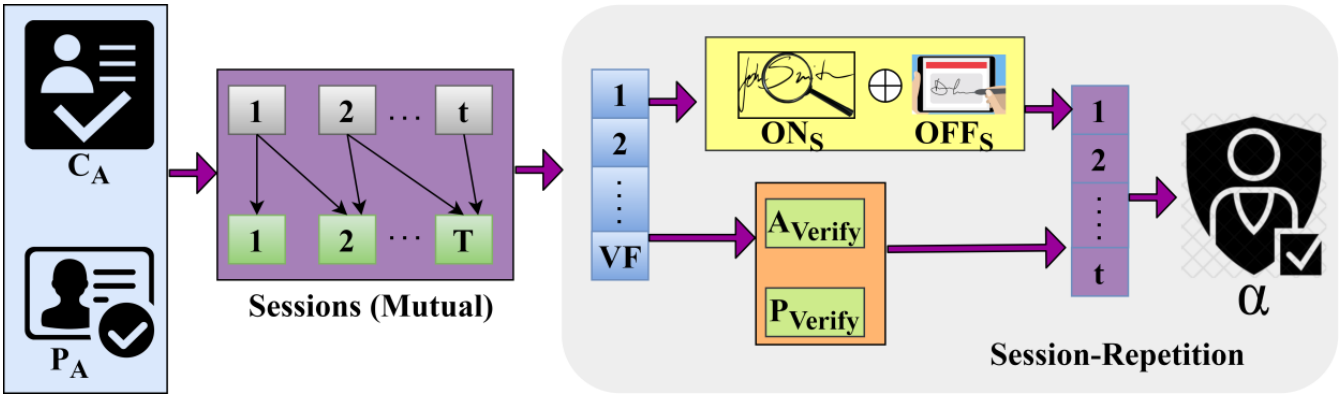

Figure 4. Information verification process.

The C_A and P_A are used for verifying the information across different $t \in T$. Therefore as per the classifications, T and VF are segregated to maximize the B_s level security. In this case, $(ON_S + OFF_s)$ are included for verifying $A\&P$ independently. This independent verification requires $ON_S + OFF_S$ provided that every t is authenticated. The process is repetitive to maximize the C_A and P_A assessments. The failure of VF is further classified for a new authenticated session (see Figure 4). The dynamic signature verification for the online and offline representation of E-signatures in the biometric system is validated utilizing the following steps: Equations (12) and (13) are computed for the online and offline signature approval, and they are substituted into the security systems and compared with the stored online/offline signatures. The two equations are again performed for the session time verification, which results in a high authentication success rate. Therefore, the application-level authentication is computed based on security metrics and digital certificates for online and offline signature approval through conventional tree classifier learning. The verification failure and complexity in biometric systems are identified to improve authentication in communications and intelligent security systems. If the dynamic signature verification is performed continuously until identifying failure or complexity in those communication systems, the same process can be repeated with different security systems and digital certificates. The verification of both online and offline authentication in remote devices and biometric systems with minimal session times is independently analyzed for each person. This continuous authentication process maximizes the success rate of E-signatures and reduces verification failures and complexity. The subsequent information of individual users is verified between the security system and the biometric devices. Digital signature verification also maximizes the authentication for online and offline signature approval without increasing the verification time and authentication lag in the biometric systems. This identification of forging activities is verified as per the above estimation equation, thereby reducing the verification failures and time. Then, the overall working process of the DSVT can be illustrated as in Table 1 follows:

Table 1. Step-by-step procedure of the DSVT.

Step 1:	Obtain inputs from users (input, biometric, and signature-type inputs)
Step 2:	Generate a digital signature for every user before accessing the information
Step 3:	Security system verifies the user's signature both offline and online using Equation (1)
Step 4:	Compute the mutual authentication/verification by generating the signature using Equations (2)–(4)
Step 5:	Validate the generated signature using Equations (5) and (6)
Step 6:	Approve the signature and biometric traits using Equations (7) and (8)
Step 7:	After performing the mutual verification, services are classified
Step 8:	Then, user-given information verification is performed
Step 9:	Finally, permission is given to the user to access the information.

4. Discussion

The proposed technique was analyzed performance-wise using data from [29]. These data provide novel digital signatures sensed from reputed mobile phones. The inputs were observed from 30 people in 3 different sessions over 15 days. Using the built-in sensors, the tilt, (x, y) position, deviation, and location features were used to identify the differences between forged and genuine signatures. The online and offline signatures were distinguished as presented in Figure 5.

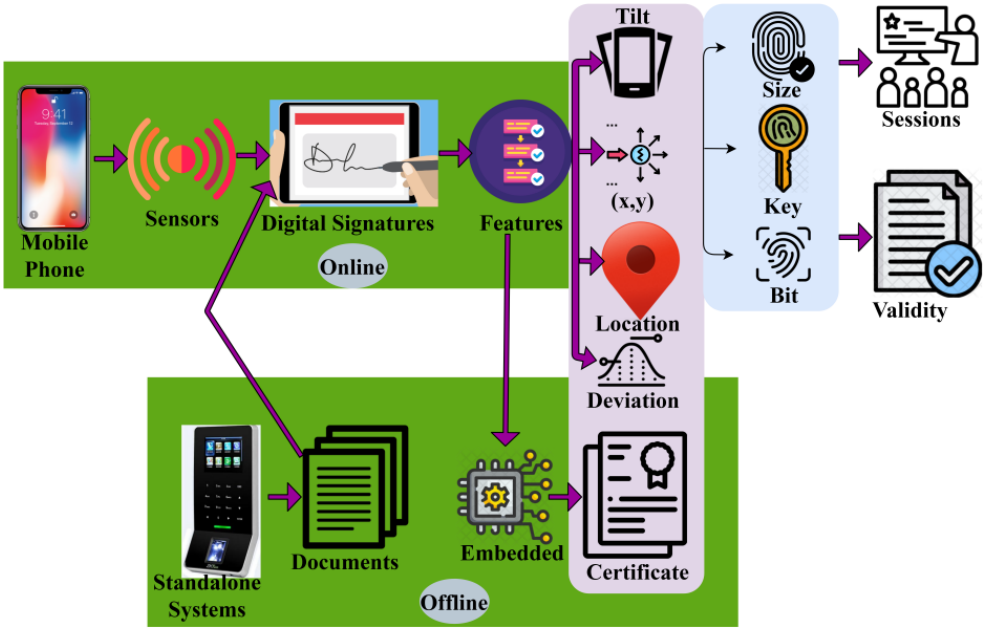

Figure 5. Distinguishing signatures.

4.1. Verification Instances and Authentication Lag

The online and offline signatures are distinguished based on their design purpose. For dynamic access (such as from mobile phones/tablets/biometrics), online signatures are used. A signed document/information is verified using offline (stored) signatures. In both cases, a digital certificate from the service provider is used for verification. For a considered session and key validity, the size and allied bits are used for verification. Following this classification, the verification instances per session are analyzed as shown in Figure 6.

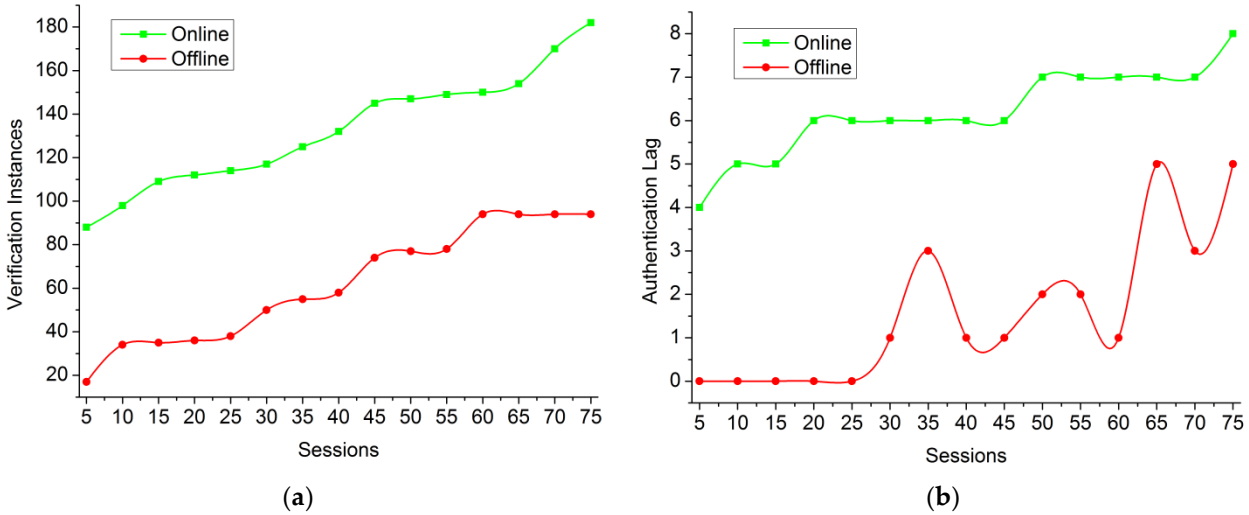

Figure 6. Verification instances and authentication lag (**a**) Verification instances Analysis for different session (**b**) Authentication lag for different sessions.

The verification instances vary with the available session based on the signature features. The tilt, position, and deviation are required to increase the number of verifications. On the other hand, the variations increase the lag in identifying a signature. The authentication lag is caused by additional certificate verification and further attribute validations. Therefore, the observed lags are suppressed through dynamic verification. This process relies on the maximum attributes available over the new sessions. Considering the security requirements, priority for the segregation mode is performed (see Figure 6). In the above analysis, the online and offline verifications are independent, using different attributes. The variations in online and inappropriate features in offline signatures were independently analyzed. This analysis is presented in Figure 7.

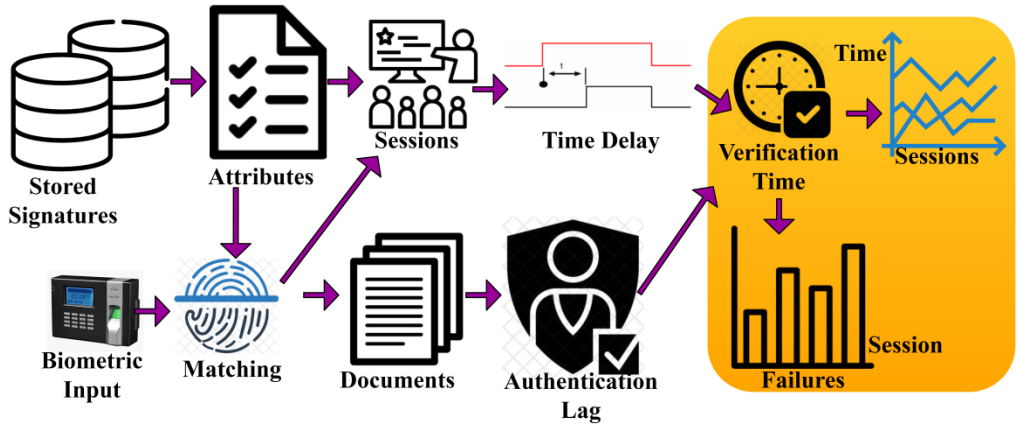

Figure 7. Independent analysis.

4.2. Mutual Time Analysis

The segregation is characterized by the verification time and failure across different sessions. Considering the combined authentication and digital signature verification, the matching between different attributes is performed. After the matching process, the authentication lag is prevented by assigning new attributes/key changeovers. The mutual time between the E_{sign} sessions was analyzed as shown in Figure 8.

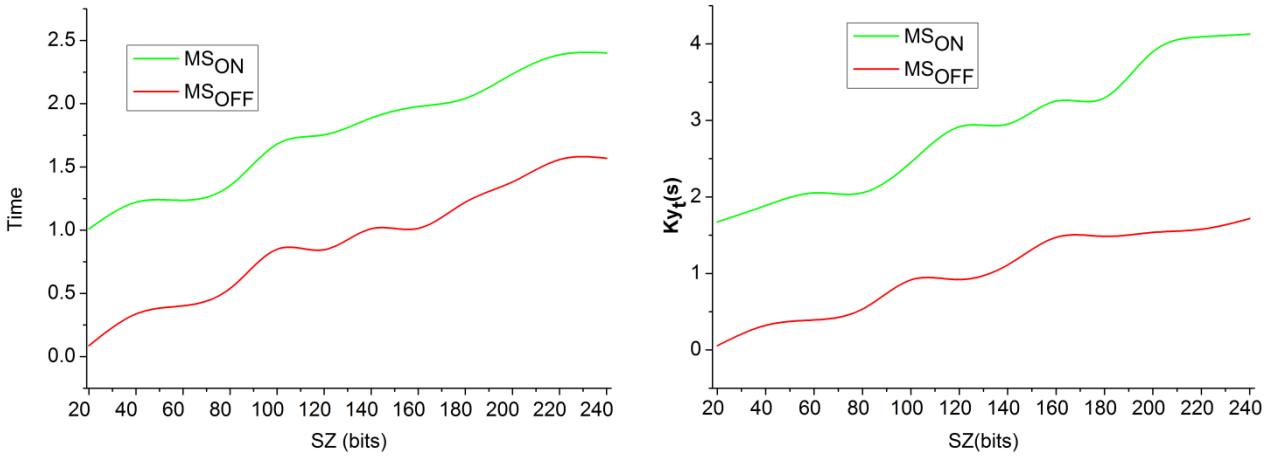

Figure 8. Mutual Time Analysis for (**a**) Different time interval (**b**) Various key.

The mutual time for authentication and verification is high for an online process compared to that for an offline process. Considering the advantages of stored sign verifications, the documents/existing features require less time. The online validation relies on the SZ and Ky_t for secure verification and for preventing failures. Therefore, the failures/sessions identify the need for implementing authentication across different processes. In the concurrent processing and verification instances, the digital certificates hold for verifying offline assessments. The assessments are increased based on the SZ classifications shown in Figure 9.

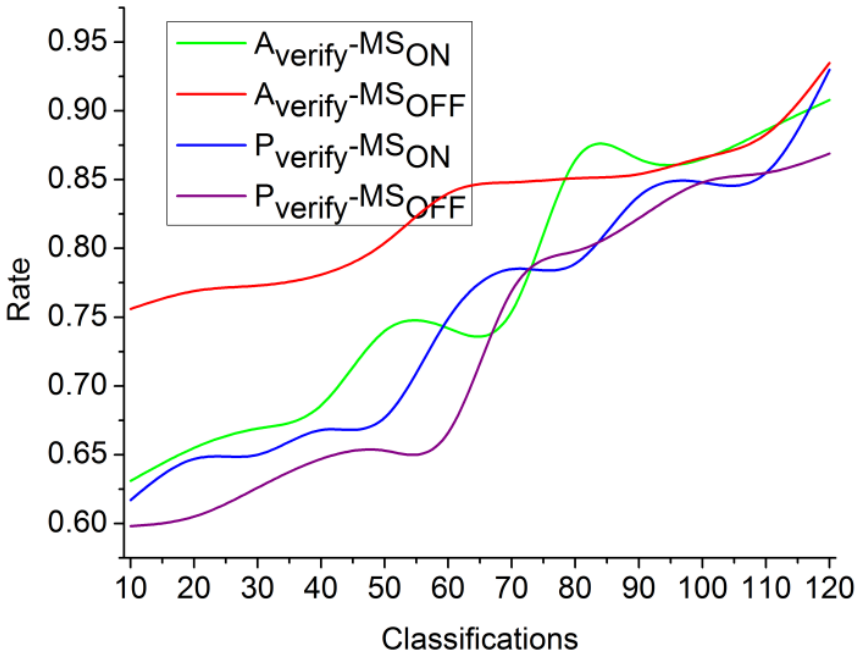

Figure 9. Assessments based on SZ classifications.

The SZ classifications are performed using A_{verify} and P_{verify} for online and offline assessments, respectively. Based on the mutual verification, the process of validation is performed for varying SZ and By_t. Therefore, as the classification increases, the validations are high, preventing false/failed authentication. Depending on the stored/new procedures, the $(VF - T)$ instances segregate the variances to improve the offline assessments. Stagnancy is observed only if the variations are high and mutual validations are prevented. In such cases, the new attributes are analyzed to retain the success rate (Figure 9).

4.3. Metric Comparisons

The metrics used for comparison were the authentication success rate, verification failure ratio, verification time, complexity, and authentication lag. The methods FV-DSV [18], MASK [24], and DeepSign [16] were used alongside the proposed technique.

4.3.1. Authentication Success Rate

This proposed technique provides a high authentication success rate for individual users' information authentication based on security systems and biometric devices, aiding in dynamic signature verification to provide certificates (see Figure 10). The verification failure and forging activities are mitigated to validate E-signatures for both online and offline representation due to different human characteristics analyzed for identification and protection using tree classifier learning and security metrics. The user's information authentication between security systems is useful for computing the verification time and authentication success rate for the condition $OFF_{SS} - A_{verify} - MCsin(\Delta)$. Authentication verification and personal verification are performed for individual users in a biometric system using physical or personal input observation from humans. The mutual session is provided for both online and offline signature verification instances. Therefore, E-signature verification is performed to augment the authentication success rate in dynamic signature verification and, hence, the security systems are also improved. From the different E-signature intervals in biometric systems through remote devices, the authentication success rate is high for protecting users' information.

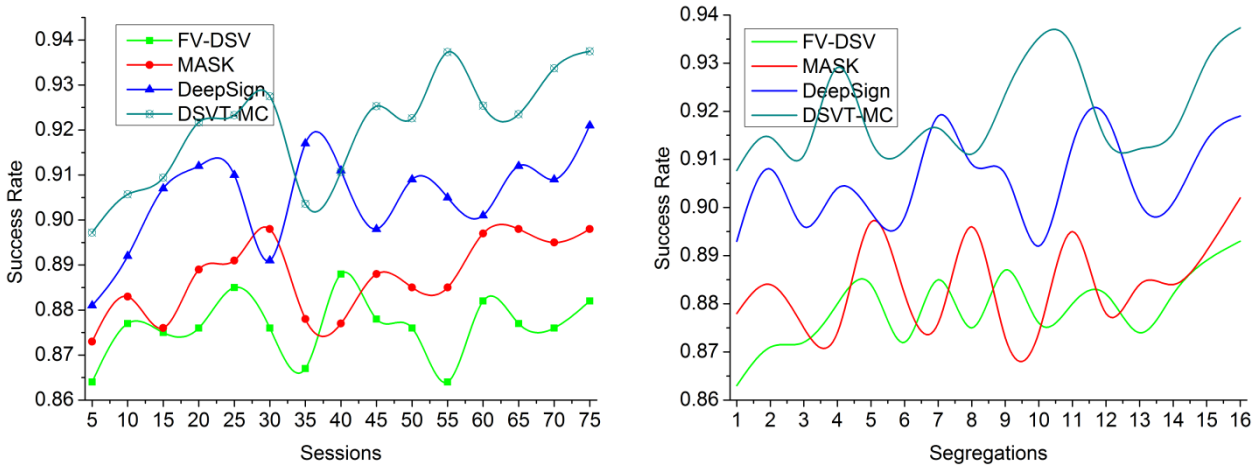

Figure 10. Authentication Success Rate for (**a**) different session rate (**b**) Segregation.

4.3.2. Verification Failure Ratio

In this proposed technique, the authentication verification failure ratio is computed to conceal users' information between the biometric systems and remote devices, without providing digital certificates during online and offline signature approval in mutual sessions. The computation of dynamic signature verification is performed to prevent adversarial forging activities, and verification failure is identified in both ON_{SV} and OFF_{SV}. This authentication is performed using security metrics such as the signing bit, key, and size for verification time intervals to validate online and offline signature authentication for appropriate instances. Based on the verification, online and offline authentication along with digital certificates is provided through biometric devices, preventing verification failures. The users' information can be concealed in two ways, namely, online and offline signatures are used for accurate digital signature verification for the available information, without increasing the verification time. The proposed technique provides certificates to store the online/offline signatures for information authentication, achieving a lower verification failure rate, as presented in Figure 11.

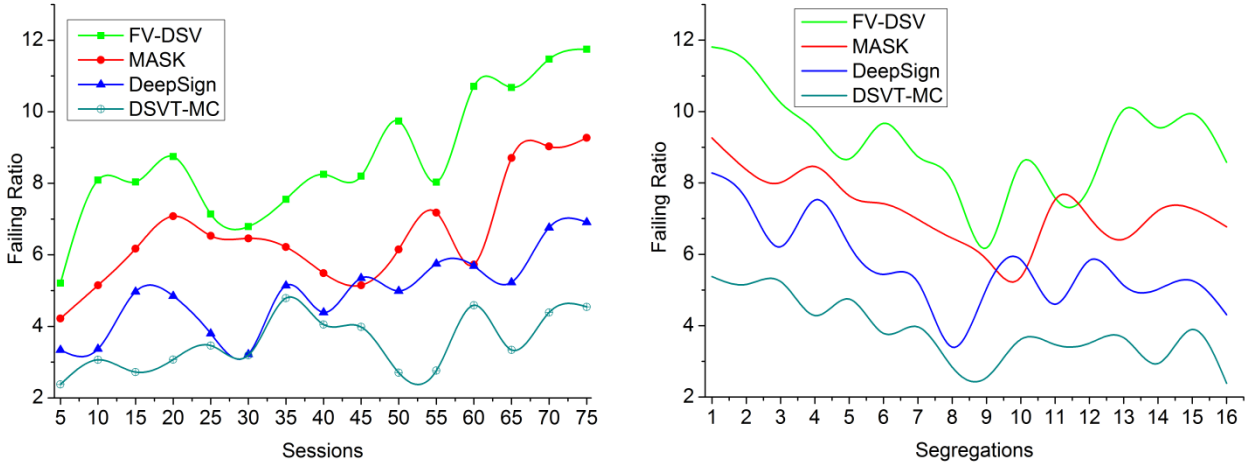

Figure 11. Verification Failure Ratio for (**a**) different session rate (**b**) Segregation.

4.3.3. Verification Time

This proposed technique achieves a reduction in the verification time for users' information authentication in both online and offline representation, as compared to the other factors represented in Figure 12. The personal verification and E-signature verification are performed to improve the dynamic signature verification in biometric systems without decreasing the responsibility of online and offline signatures during information authentication with the security systems. This is an important consideration for preventing failures through $\frac{1}{C_A+P_A}\left[-A_{verify}ON_S/OFF_S - \alpha\Delta T - MCXsin(\Delta) + MCC_Acos(\Delta)\right]$ performed at different time intervals. The security system is responsible for both online and offline signature approval verification and is validated to provide accurate E-signature verification, preventing forging activities. If the extracted user information and its security features are copied by the attackers, the system ensures that digital signature verification in the biometric systems is retained using signing size (SZ), key (ky), and bit (Bt) analysis to reduce the verification failure and time, as per the equations. Therefore, the security systems provide digital certificates to the unique users for information authentication in biometric systems for online or offline representation at different digital signing time intervals through classifier learning and security metrics to compute the accurate E-signature verification in less time.

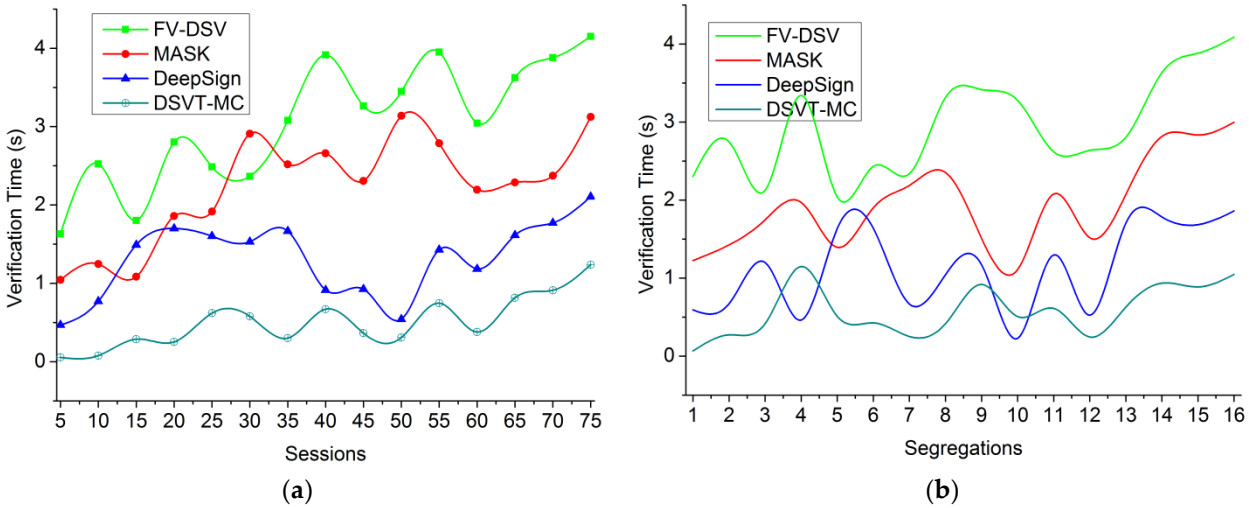

Figure 12. Verification Time for (**a**) different session rate (**b**) Segregation.

4.3.4. Complexity

This proposed technique achieves less complexity compared to the other factors, as represented in Figure 13. The individual users' information authentication approval and verification are performed through remote devices based on the advancement in communication and intelligent security systems, and biometrics are used to reduce the computational complexity of E-signatures. This E-signature is responsible for online and offline authentication by prolonging and observing human information that is used for providing authentication. The mutual sessions' authentication verification is computed for online and offline signature approval between the ensured biometric devices and security systems. The mutual session timing is computed for the user's information authentication, and the communication per interval in the biometric systems is again signed using $-MS_{ON}A_{verify} - VF - T$ and $-MS_{OFF}E_{sign} - VF - T$ validation, as shown in Equations (14) and (15). Hence, the dynamic signature verification for user information authentication under classifier learning prevents verification failures and reduces communication. From this user information, privacy and security metrics are processed under various conditions to reduce the verification time.

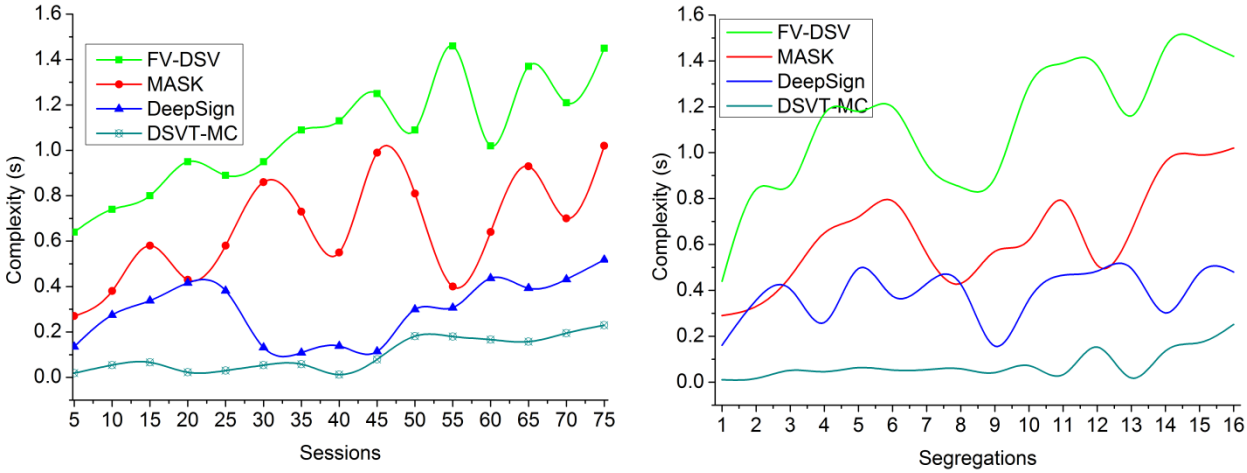

Figure 13. Complexity Analysis for (**a**) Different Session (**b**) Segregation.

4.3.5. Authentication Lag

This proposed technique reduces the authentication lag for concealing individual user information using biometric devices and security systems that are responsible for online and offline signature approval. The accurate information authentication provided in the biometric system using classifier learning is depicted in Figure 14. This technique supports communication and real-time application for securely processing and exchanging information, and it reduces the verification failure and time by estimating $ON_S = A_{verify} + v\alpha_t - VF$ and $OFF_S = P_{verify} + v\alpha_t - VF$. In this authentication verification process, the forging activities at the time of digital signing are addressed due to changes in security metrics, and certificates during communication are identified to prevent failures and complexity. This observed human information is concealed between the biometric devices and security systems, wherein the various digital signing intervals are performed using Equations (12) and (13) for validation. This validation is based on online and offline signature authentication by verifying the individual user's personal and physical information for successive authentication in biometric systems. Based on this authentication verification in mutual sessions, the authentication lag is reduced. In Tables 2 and 3, the above comparative analysis is summarized.

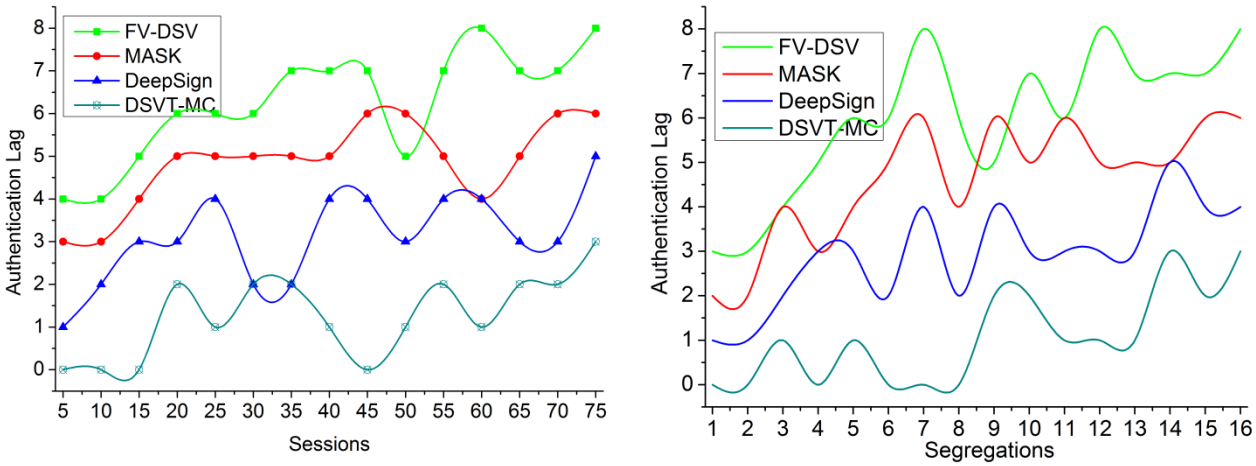

Figure 14. Authentication Lag for (**a**) different session (**b**) Segregation.

Table 2. Comparative analysis summary (sessions).

Metrics	FV-DSV	MASK	DeepSign	DSVT-MC
Success Rate	0.882	0.898	0.921	0.9375
Failure Ratio	11.75	9.27	6.91	4.544
Verification Time (s)	4.152	3.124	2.105	1.2379
Complexity (s)	1.45	1.02	0.518	0.2299
Authentication Lag	8	6	5	3

Table 3. Comparative analysis summary (segregations).

Metrics	FV-DSV	MASK	DeepSign	DSVT-MC
Success Rate	0.893	0.902	0.919	0.9373
Failure Ratio	8.58	6.77	4.31	2.386
Verification Time (s)	4.089	2.996	1.86	1.0467
Complexity (s)	1.42	1.02	0.48	0.2513
Authentication Lag	8	6	4	3

The proposed technique increases the success rate by 11.15% and reduces the failure ratio by 9.53%, verification time by 10.09%, complexity by 12.82%, and authentication lag by 8.82%.

The proposed technique increases the success rate by 9.79% and reduces the failure ratio by 8.33%, verification time by 10.82%, complexity by 12.37%, and authentication lag by 8.3%.

5. Conclusions

This article introduced a dynamic signature verification technique through mutual compliance for biometric device authentication. The proposed technique performs online and offline verification and authentication using dedicated segregations. In this technique, classifier learning is used to segregate the online and offline signature features, e.g., direction, pattern etc. The identified attributes are used for signature verification, mutual session verification, and approval. In the signing process, the key size, signing bit, and signing keys are computed. Based on the computation, digital certificates and signatures are used to improve the authentication success rate. Considering the classification through

varying personal and attribute authentication and verification, the approval for a person or document in online and offline modes is provided. Therefore, signature verification relies on stored and current information across multiple features to maximize the success rate. As the approval is recurrently validated based on the sessions, the complexity is reduced compared to the non-mutual sessions. Therefore, the authentication lag is reduced across multiple concurrent sessions. From the experimental analysis, it can be seen that the proposed technique increases the success rate by 11.15% and reduces the failure ratio by 9.53%, verification time by 10.09%, complexity by 12.82%, and authentication lag by 8.82% for the varying sessions compared to the FV-DSV method. In future, the authentication could be improved by including the optimized model-based biometric verification process.

Author Contributions: Conceptualization, J.H. and Y.X.; methodology, L.L.; formal analysis, J.H.; investigation, J.H.; writing—original draft preparation, Y.X.; writing—review and editing, L.L.; visualization, L.L.; supervision, J.H.; project administration, J.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

References

1. Stylios, I.; Kokolakis, S.; Thanou, O.; Chatzis, S. Behavioral biometrics & continuous user authentication on mobile devices: A survey. *Inf. Fusion* **2021**, *66*, 76–99.
2. Wang, P.; You, L.; Hu, G.; Hu, L.; Jian, Z.; Xing, C. Biometric key generation based on generated intervals and two-layer error correcting technique. *Pattern Recognit.* **2021**, *111*, 107733. [CrossRef]
3. Dwivedi, R.; Dey, S.; Sharma, M.A.; Goel, A. A fingerprint based crypto-biometric system for secure communication. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 1495–1509. [CrossRef]
4. Mehraj, H.; Mir, A.H. A multi-biometric system based on multi-level hybrid feature fusion. *Her. Russ. Acad. Sci.* **2021**, *91*, 176–196. [CrossRef]
5. Farooq, H.; Naaz, S. Performance analysis of biometric recognition system based on palmprint. *Int. J. Inf. Technol.* **2020**, *12*, 1281–1289. [CrossRef]
6. Okawa, M. Online signature verification using single-template matching with time-series averaging and gradient boosting. *Pattern Recognit.* **2020**, *102*, 107227. [CrossRef]
7. Alpar, O. Signature barcodes for online verification. *Pattern Recognit.* **2022**, *124*, 108426. [CrossRef]
8. Najda, D.; Saeed, K. Impact of augmentation methods in online signature verification. *Innov. Syst. Softw. Eng.* **2022**, 1–7. [CrossRef]
9. Tsourounis, D.; Theodorakopoulos, I.; Zois, E.N.; Economou, G. From text to signatures: Knowledge transfer for efficient deep feature learning in offline signature verification. *Expert Syst. Appl.* **2022**, *189*, 116136. [CrossRef]
10. Batool, F.E.; Attique, M.; Sharif, M.; Javed, K.; Nazir, M.; Abbasi, A.A.; Iqbal, Z.; Riaz, N. Offline signature verification system: A novel technique of fusion of GLCM and geometric features using SVM. *Multimed. Tools Appl.* **2020**, 1–20. [CrossRef]
11. Malik, J.; Elhayek, A.; Guha, S.; Ahmed, S.; Gillani, A.; Stricker, D. Deepairsig: End-to-end deep learning based in-air signature verification. *IEEE Access* **2020**, *8*, 195832–195843. [CrossRef]
12. Sadak, M.S.; Kahraman, N.; Uludağ, U. Dynamic and static feature fusion for increased accuracy in signature verification. *Signal Process. Image Commun.* **2022**, *108*, 116823. [CrossRef]
13. Guerra-Segura, E.; Ortega-Pérez, A.; Travieso, C.M. In-air signature verification system using leap motion. *Expert Syst. Appl.* **2021**, *165*, 113797. [CrossRef]
14. Yapıcı, M.M.; Tekerek, A.; Topaloğlu, N. Deep learning-based data augmentation method and signature verification system for offline handwritten signature. *Pattern Anal. Appl.* **2021**, *24*, 165–179. [CrossRef]
15. Longjam, T.; Kisku, D.R.; Gupta, P. Multi-scripted Writer Independent Off-line Signature Verification using Convolutional Neural Network. *Multimed. Tools Appl.* **2022**, 1–18. [CrossRef]
16. Tolosana, R.; Vera-Rodriguez, R.; Fierrez, J.; Ortega-Garcia, J. DeepSign: Deep on-line signature verification. *IEEE Trans. Biom. Behav. Identity Sci.* **2021**, *3*, 229–239. [CrossRef]

17. Bassit, A.; Hahn, F.; Peeters, J.; Kevenaar, T.; Veldhuis, R.; Peter, A. Fast and Accurate Likelihood Ratio-Based Biometric Verification Secure against Malicious Adversaries. *IEEE Trans. Inf. Secur.* **2021**, *16*, 5045–5060. [CrossRef]
18. Ponce-Hernandez, W.; Blanco-Gonzalo, R.; Liu-Jimenez, J.; Sanchez-Reillo, R. Fuzzy vault scheme based on fixed-length templates applied to dynamic signature verification. *IEEE Access* **2020**, *8*, 11152–11164. [CrossRef]
19. Yang, W.; Wang, S.; Kang, J.J.; Johnstone, M.N.; Bedari, A. A linear convolution-based cancelable fingerprint biometric authentication system. *Comput. Secur.* **2022**, *114*, 102583. [CrossRef]
20. Parcham, E.; Ilbeygi, M.; Amini, M. CBCapsNet: A novel writer-independent offline signature verification model using a CNN-based architecture and capsule neural networks. *Expert Syst. Appl.* **2021**, *185*, 115649. [CrossRef]
21. Okawa, M. Time-series averaging and local stability-weighted dynamic time warping for online signature verification. *Pattern Recognit.* **2021**, *112*, 107699. [CrossRef]
22. Dhieb, T.; Boubaker, H.; Njah, S.; Ben Ayed, M.; Alimi, A.M. A novel biometric system for signature verification based on score level fusion approach. *Multimed. Tools Appl.* **2022**, *81*, 7817–7845. [CrossRef]
23. Naz, S.; Bibi, K.; Ahmad, R. DeepSignature: Fine-tuned transfer learning based signature verification system. *Multimed. Tools Appl.* **2022**, *81*, 38113–38122. [CrossRef]
24. Yang, X.; Zhu, H.; Wang, F.; Zhang, S.; Lu, R.; Li, H. MASK: Efficient and privacy-preserving m-tree based biometric identification over cloud. *Peer—Peer Netw. Appl.* **2021**, *14*, 2171–2186. [CrossRef]
25. Houtinezhad, M.; Ghaffari, H.R. Off-line signature verification system using features linear mapping in the candidate points. *Multimed. Tools Appl.* **2022**, *81*, 24815–24847. [CrossRef]
26. Roy, S.; Sarkar, D.; Malakar, S.; Sarkar, R. Offline signature verification system: A graph neural network based approach. *J. Ambient. Intell. Humaniz. Comput.* **2021**, 1–11. [CrossRef]
27. Tan, H.; He, L.; Huang, Z.C.; Zhan, H. Online signature verification based on dynamic features from gene expression programming. *Multimed. Tools Appl.* **2021**, 1–27. [CrossRef]
28. Saleem, M.; Kovari, B. Online signature verification using signature down-sampling and signer-dependent sampling frequency. *Neural Comput. Appl.* **2021**, 1–13. [CrossRef]
29. Available online: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7725742/ (accessed on 25 September 2022).