electronics

MDPI

Article

Surgery Agreement Signature Authentication System for Mobile Health Care

Jun-Ho Huh

Department of Data Informatics, Korea Maritime and Ocean University, Busan 49112, Korea; 72networks@kmou.ac.kr

Received: 2 May 2020; Accepted: 23 May 2020; Published: 27 May 2020

Abstract: Currently, the use of biometric systems is increasing following the increase in the non-face-to-face security transactions in the Health Care sector, where smart devices are extensively used. Additionally, hospital patients or their guardians had to sign every medical/surgery consent form with a pen. Currently, hospitals are attempting to digitalize the form to avoid its loss or delay to the operating room. Thus, this study proposes a surgery consent signature authentication system for the mobile health care system. Along with the vein or the fingerprint recognition technology, the smart electronic signature recognition technology is regarded as a new type of security solution for Mobile Health Care, which is a compound of Health Care and technology, or a smart contents and display technology. Thus, this study proposes a surgery agreement signature authentication system for Mobile Health Care while using the techniques, such as database segment units comparison in the cloud, Bag of Word, etc. The proposed system was implemented with Java language and developed in a way the reference signature stored in advance in a cloud database to be compared with the signature currently entered. For the comparison, the segment matching, spatial pyramid matching, and boundary matching techniques were used in addition to the Dynamic Time Warping (DTW) algorithm. Additionally, the system has been made lighter than the existing experimental products, so that it is easier to embed the system into a smart phone, tablet, or others. The Test Bed experiment result showed that the system operated flexibly.

Keywords: signature; handwritten signature; surgery agreement signature; authentication; mobile health care; Java Android

1. Introduction

It has been compulsory for the patients or guardians to sign all of the paper consent forms in person but the hospitals are now ready to digitalize this process to avoid any possibility of misplacement or delivery delays to the operating room. In this aspect, this study introduces a digital signature authentication system that is exclusive to mobile health care service.

As such, there are many recent attempts to digitalize the patient consent form prior to surgery [1]. At the same time, as the problems concerning the security of personal information when the patients are filling in the form have become an issue, other types of authentication systems using individual physical features are being developed [1]. One of them is biometrics, which is a technology to identify a person by analyzing the different features of users have [2,3]. Biometrics technology includes signature, fingerprint, voice, iris, vein, and face recognitions. This study proposes a surgery consent signature authentication system for the mobile health care system that is based on a digital forensics methodology to improve the analysis method and security of signature recognition systems.

The electronic signature is a sort of a smart content that is processed with a simple interface, rather than the complex ones, and it can be defined as intelligently personalized content [1–3]. The smart

contents should be quickly provided for the customers who are in the process of purchase or a first time visitor [4,5].

The phrase "complex ones" mentioned here refers to all sorts of authentications, such as verifying oneself, validating the location information, address of a credit card user, and/or a Card Verification Code (CVC) number, similar to the ones that are being used for the current electronic payment systems. Signature is a traditional tool of confirming one's own intention and the signatures written with an electronic pen are also currently being used to authenticate a person at the court. A variety of technologies are available for authenticating the signatures and especially for the electronic signatures, a special algorithm is being used along with the handwriting forms stored in the existing DataBase (DB).

Authentication methods that use individual characteristics are being developed due to the development of digital technologies and the emergence of security problems concerning personal information. One of them is biometric technology (biometrics), which distinguishes individuals by analyzing their different characteristics. Biometrics includes signature, fingerprint, voice, iris, face, and vein recognitions [5,6].

This paper is organized, as follows: Chapter 2 discusses some of the related research works followed by the discussion on the method of signature data extraction in Chapter 3. Subsequently, Chapter 4 deals with "Analysis of Signature Data", whereas Chapter 5 reveals the prototype while discussing about system implementation and related considerations. Meanwhile, Chapter 6 explains the significance of the proposed system in comparison to the other research works along with interesting debates. Finally, Chapter 7 concludes the research.

2. Related Research

The management expense for various types of consent forms or other documents used at the hospitals have been increasing due to increased duty hours, use of huge quantity of papers and their storage in the process of form completion, processing or management. Additionally, there are issues involving personal information leaks, inefficiencies in the business process, and/or incurring of unnecessary costs. The hospital electronic consent solution proposed by FORSC [4] can largely improve the business process by transforming various types of consent forms, such as medical checkup or surgery consent forms, etc., into an electronic document. With this solution, a patient can receive the explanations about checkup, procedure, or surgery plan for him/her to consent through the tablet PC carried by the medical staff. After the patient electronically signs the document, it will be stored in the hospital's internal document server automatically. It is expected that the reliability and level of hospital service will be improved by creating such a medical environment.

Meanwhile, the hospital electronic consent system for a surgery or medical check offered by BIT Computer [5] is a solution that allows a customer to complete the electronic consent form shared with the medical staff on a tablet PC or mobile device monitor by using an electronic pen. The form can be simultaneously implemented on either device's monitor for signing so that both parties can reduce the time usually required for them to fill out the paper consent form significantly, increasing the customer convenience.

The major functions are as follows: first, assisting the patient to easily complete the form on a tablet PC or monitor as if he/she is writing on a paper; second, establishing a medical information system link. Third, achieving synchronization between the hospital ward and administration on a patient device screen to allow the person in charge to check the form filled in on the tablet PC monitor; and, the last, implementing an electronic authentication or encryption module of a template file. Figure 1 shows the workflow of the electronic solution provided for medical checkups or surgeries.

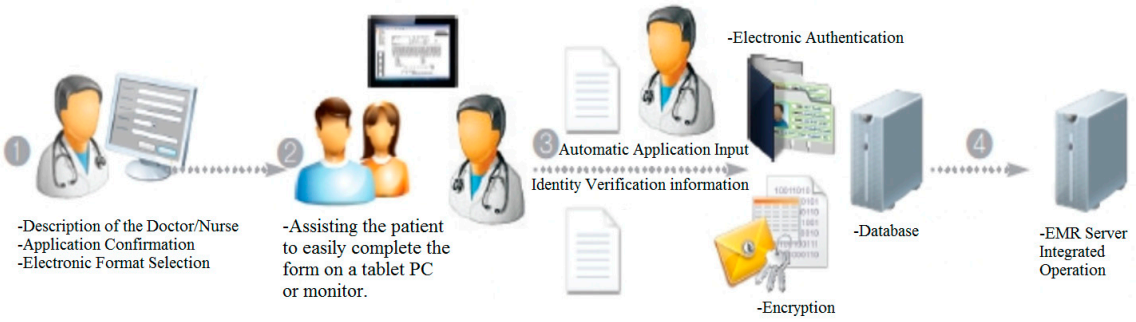


Figure 1. The workflow of the electronic solution provided for medical checkups or surgeries.

Currently, various types of biometric techniques are being studied or applied and one of them is a technique that uses the iris or retina pattern, it has been known that they are different, even between twins, and do not change for a lifetime, unless a person gets seriously injured or be diseased in his/her eye. The retina recognition technique is one that uses the characteristic of a rear capillary vessel that it does not change during one's entire life like a fingerprint [6–8]. One of the merits of this technique is that it has more attributes that the fingerprint, but, as the user has to get very close to the retina scanner, it is not received well by the users. The iris recognition technique is one that authenticates the user based on a doughnut-shaped iris pattern located between the pupil and the white. The advantage of this technique is that the pattern can be captured with a camera from the distance of approximate one meter. It is possible to identify a person just by comparing 1/3 of the stored code information since every person has a different iris pattern. In this regard, the security of this technique stands out among the currently available biometric techniques. However, it is quite hard to miniaturize its equipment, so that its commercialization or generalization is also difficult. Another demerit is that the system can be much more expensive than the others.

The hand geometry recognition is the first automated technique among the biometric techniques, which is based on the observation that the lengths of fingers of the individual person are different. Currently, the analysis of digitized finger shapes involves not only their lengths, but also other various features. This technique facilitates real-time processing due to its simplicity and the requirement of lesser throughput but it also has a problem of low accuracy. This technique has been used to identify a suspect who has left no fingerprints, but only the palm print and its application to the other areas is still being researched [9,10].

The vein recognition is a security technology that is based on the fact that the vain pattern in the back of the hand or the wrist varies in each person as the fingerprints. One of its merits is that a relatively good image can be obtained, even from the simple injuries or the contaminations caused by the light-transmitting substances. Additionally, the security level of this technique is quite high, as veins are almost impossible to copy. However, an infrared light and an optical filter are often used to acquire a vascular image, but it is not easy to extract the area where the veins are being distributed from the back-hand skin, not to mention the complexity that is involved in organizing it the system hardware. Despite such difficulties, Lotte Data Communication Company has succeeded in applying this technique to a Seven Eleven convenient store as a test bed experiment. The face recognition can be regarded as the most natural biometric technique, as people mostly use the facial patterns to recognize the others. However, it is necessary that only the facial part should be separated for the recognition process but most of the time, people's faces are not stationary so that the separation process can be quite difficult. For the recognition of a face, a feature-point-based method where a thermal image of facial vessels is captured with an infrared camera or the Principal Component Analysis (PCA)-based method that uses a 3D facial image is being currently used. The expected area where the face recognition technology will be used widely is the robotic technology-based agent service. The robots can identify the people with this technology and take appropriate actions, or provide a customized service of

searching the scenes where a particular person appears in the news programs. This technique is being used by iPhone 10 and the People's Republic of China's Tenhwang project [10].

The voice recognition is a technique that identifies a person or a linguistic meaning by comparing a speech with the voice data stored in the database after converting the voice characteristics, such as dynamics or tone of a sound. Currently, this technique is being used for the name or word-based automatic dialing service, voice-activation program for computer commands, basic note-taking, and internet access, as well as the voice-recognizing IBM OS/2 Warp. However, one's voice could change later due to his/her health condition (e.g., heavy cold, laryngitis, etc.), or the surrounding noises may affect the system. Additionally, there would be a problem of intentional voice change or deliberate imitation of other's voices, causing the recognition level to drop. Such problems are yet to be solved.

Since the start of human beings using the letters, the signature is a sort of agraphic-based biometric system that has long been used. People still write their names on documents, music scores, pictures, sculptures, or handicrafts. There are to major methods: the offline method where a signature is being optically captured by the scanner or the camera and then compared through the analysis and the online method, where the dynam characteristics of the signature, such as the movement, speed, and pressure, are analyzed while one is entering his/her signature on an electronic pad. Clearly, the most widely known disadvantage of this technology is that an expert forger can easily forge one's signature. For this reason, when requiring a high-level security, it will be safer to use the other recognition technology (s) such as the ones that are mentioned above. Thus, a system where one's signature information is first stored in the cloud database to compare with the currently signature is implemented with Java in this study.

In the majority of cases, the signature verifications that were performed during the last few decades were either an offline or an online approach and, recently, the automatic handwritten signature verification system that verifies the authenticity of signatures used for Australian passports was introduced to prevent identity fraud or theft. The fuzzy modeling method was used when developing this system to achieve a more accurate recognition [11,12]. At the same time, the hybrid handwritten signature verification system that compares signatures with the reference data was also developed. The signature data that were acquired by the digitizing tablet were then used for the segmentation process for the offline-scanned data (signature) for comparison [13].

Meanwhile, another signature verification system that extracts a variety of the static signature features, such as height, slant, and others, along with dynamic features, including velocity, pen-tip pressure, and a few other necessary data to train network topologies has been introduced [14]. In [15], the signature verification system employing a hidden Markov model to represent and verify the signature data is described. The instrumented data gloves mounted with sensors to detect finger bend, hand position, and orientation are used for verification [16].

In [17], an automatic signature verification system that relies on the global features that summarize various aspects of the shape of a signature together with the dynamics of signature production is discussed. Meanwhile, the signature recognition algorithm that focuses on the pixel-to-pixel comparisons while using extensive statistical analysis, standard deviation, variance, and the theory of cross-correlation is outlined in [18]. The verification system that recognizes signatures with online reference data acquired with a digitizing tablet and three other classification schemes is described in [19].

The improved level of signature forgery verification systems is described in [20], whereas the criterion of an improved signee registration using the entropy measure against online genuine signatures is presented in [21]. The online dynamic signature verification system that employs a set of 49 normalized features that tolerates inconsistencies in a genuine signature and retains the power to distinguish forgeries is explained in [22]. The statistical quantization mechanism that mitigates subtle intra-class variations in signature features to distinguish the differences between genuine and fake signatures is described in [23].

The algorithm of the online signature verification system that employs the two-level verification approach that extracts the wavelet features and uses the neural network recognition has been proposed in [24], whereas the dynamic signature verification system that uses the wavelet transformation for the back propagation neural network is described in [25]. The other online signature verification systems that are based on the local information time functions are also described. The discrete one-dimensional (1D) wavelet transformation is performed with these properties in mind [26]. The Discrete Wavelet Transform (DWT), which achieved a higher verification rate than the time-domain verification system in extracting distinctive features from the signatures, is reported in [27,28]. Using the DWT as a signature feature extraction tool has been studied in several previous studies [24–28], where the DWT was performed for the genuine signatures but not for the skilled forgeries. Additionally, these studies did not offer any effective forgery detection solutions.

When the signature recognition technology is examined from the device perspective, there are methods of using touch screen or tablet PC, or by using the position information of the hand by attaching an inertial sensor to the wrist. The machine learning algorithm that is mainly used for sign recognition includes a Hidden Markov Model (HMM) [29], which uses a chain code, and a Support Vector Machine (SVM) [30], which classifies two classes and finds a classification boundary that maximizes margins. HMM is problematic, in that it cannot apply newly proposed features. Since SVM is basically a binary classifier, it is complicated to implement when it is expanded to a multi-class classifier. Instead of analyzing each signature one by one, this paper uses all of the algorithms to analyze the signature over several steps. In doing so, it was discovered that applying various algorithms can improve the accuracy more than analyzing the signature through only one algorithm and, moreover, that algorithms with good recognition rates may differ by the type of signature. Therefore, the cloud database is designed and implemented for the algorithm to be intelligently selected using an intelligent agent [31] for efficient application.

Thus, in this paper, the methods, such as segmentation, spatial pyramid matching, and boundary matching, were used to analyze the signatures instead of using the famous signature analysis tool Dynamic Time Warping (DTW) algorithm. Additionally, instead of applying these algorithms to the targeted signature separately, all of them were used together in each different analysis stages.

The result showed that such a method had increased the accuracy but the individual recognition rates were different, depending on the forms of signatures. For this reason, the system was designed and implemented in a way that the cloud database will find a suitable algorithm and interact with it efficiently. That is, instead of proposing a new algorithm, this signature authentication system was implemented in a way that the digital signing process will interact with the algorithms associated with the signature recognition technology.

3. Signature Data Extraction

Among these methods, the focus was laid on the analysis method used for recognizing the signatures. Many research studies have been conducted for signature recognition technology in the past, but they are rarely being used at present, since they are vulnerable to forgeries. Thus, instead of a popular existing authentication method that uses a DTW method, an attempt was made to test a new signature recognition method by applying the segmental units comparison and Bag of Word methods, followed by its comparison with the DTW method.

The analysis of a signature is largely performed through three steps. First, calculate the average time that is required to write a signature based on its length by measuring the required time several times, and then compare it with a new value entered. Second, store the signature's stroke ordering in the database to compare with a new value. Third, impose the signature over a grid and check how much the signature coordinates are contained in each section, regardless of the size of signature. Subsequently, by converting the results into percentages, compare them with the new values.

A database that manages the signature information will be constructed by developing a signature-input application in order to generate an ideal comparison value through sufficient learning time and then acquiring a sample signature for authentication purpose through three steps.

3.1. Development of Database and Application

The Android Studio-supported SQLite was used for the database that stores the data values of a baseline signature. Additionally, tables that use individual algorithms were separately created to receive coordinate values. The application that receives signatures and stores values was developed with Android Studio. This application stores the obtained coordinate values based on the signature-writing time with the timer once the signature has been entered using the touch function of a smart phone. Moreover, in addition to coordinates, the picture of the signature will be stored in the internal storage of the same smart phone to show detailed differences between the stored signatures. The differences can be checked with pictures; at the same time, the concordance rate (%) between the used algorithms will be represented with a pie graph.

3.2. Preprocessing

In order to use stored coordinates for the analyses, they must go through a preprocessing process that minimizes the variations in the signatures that are caused by slippery surface or the signer's hand-shaking. This process includes a sampling process that improves the comparison processing speed when there are too many coordinates for the received signature by taking a single sample coordinate in a given number of coordinates. The normalization process is another process involved, which minimizes the changes in the signature's shape size and inclination.

The number of coordinates should be arranged to be similar to that before so that the coordinate values are normalized against the time taken to write the signature. Furthermore, since each signature size may vary, an operation called generalization, which makes the sizes of signatures similar to each other, will be performed. In this process, the size of the signature is determined based on the largest and smallest values on the X-axis and Y-axis, and then the signature is delivered after its segmentation.

4. Analysis of Signature Data

4.1. Development of Database and Application

Stable segmental matching can be performed when matching the peaks and valleys in each section by setting the dominant peak as a baseline cut-point. In this case, the objective was to find the comparison values by performing segment matching for each section after creating a graph by calculating the displacement values at regular intervals for the signature's X and Y coordinates and designating three dominant peaks P1, P2, and P3 (i.e., Partitioning Peak Points: PPP) [32].

4.2. Segmental Matching for Peaks

The number of peaks and valleys between different sections can be obtained by separating the sections based on cut-points P1, P2, and P3 (dominant peaks), as calculated above. First, the differences in these numbers were calculated by comparing them for each signature. Next, the differences in the time zones where peaks and valleys had been generated were compared. It was possible to determine the concordance rates (%) based on the results obtained from these two steps. Figure 2 shows the implementation of graph using sectional peaks.

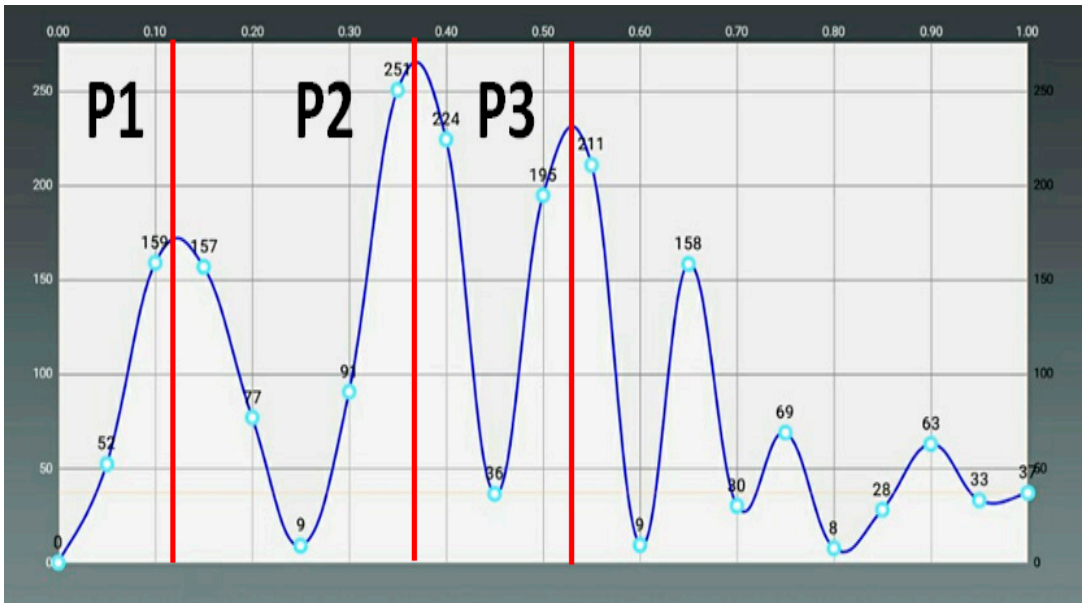


Figure 2. Implementation of graph using sectional peaks.

4.3. Spatial Pyramid Matching

The spatial pyramid matching method involves first segmenting an image into several levels of resolution, and then computing each segment's histogram to conduct an overall comparison [32,33]. The picture on the right (level 0) corresponds to the traditional Bag of Words method that calculates one histogram for a whole image. On the other hand, spatial pyramid matching segments an image step-by-step (e.g., 2×2 for level 1 and 4×4 for level 2), and it then computes a separate histogram for each segment. All of the histograms are finally added up to form a pyramid-like shape, wherein the histograms will be compared to each other to estimate the similarity between the two images. Let us designate the histogram computed for level 0 as h0 and the histograms for level 1 in order of h1_0, h1_1, h1_2, and h1_3 in order to detail the similarity estimation for the input image. The same process is taken for level 2, where the histograms will be lined up as h2_0, h2_1, ..., h2_15. The histograms can be computed for the higher levels if necessary. Now, if the histograms computed for the model image (i.e., a pre-trained image) have been designated as h0′, h1_0′, h1_1′, ..., h2_15′, find the level of similarity between h0 and h0′, h1_0 and h1_0′, and so on for each corresponding pair. Finally, aggregate all of the results; the similarity between the input image and the model image can be estimated. Here, the similarity that is measured at the higher levels (i.e., more segments) will be weighted more, so that a higher grade will be given, since the spatial (position) data in a feature distribution have been maintained better.

This method was originally used for image processing, which analyzed the spatial proportion of a certain shape or picture in a space, but in this research, the same method was employed for recognizing a signature by distinguishing the spaces as an empty part (without any stroke) or a black part (with a stroke). Figure 3 shows the segmentation in spatial pyramid matching [33].

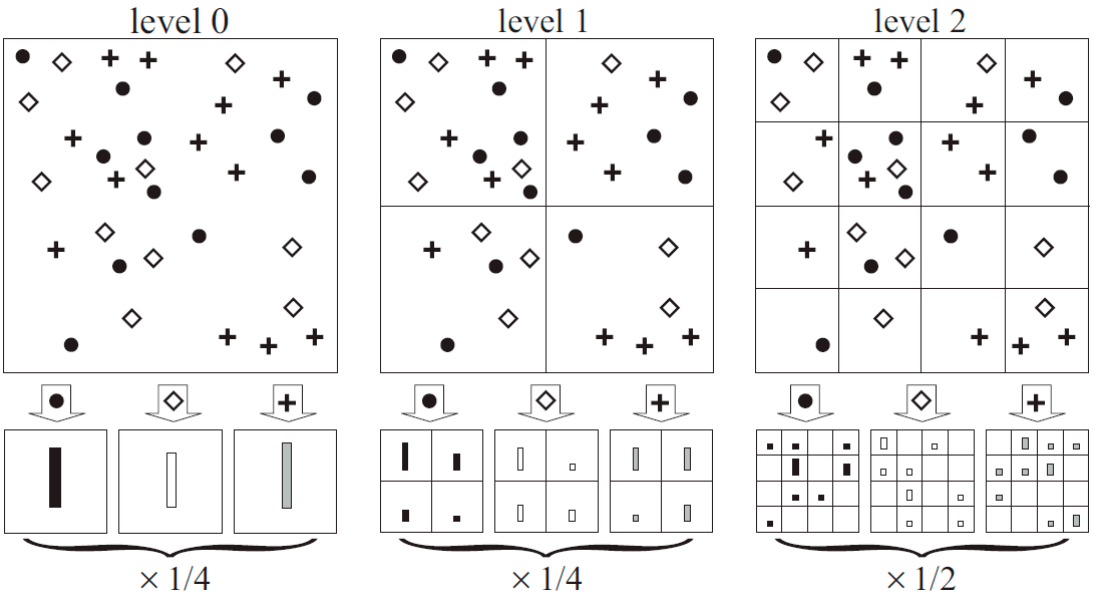


Figure 3. Segmentation in spatial pyramid matching.

4.4. Stroke Order Matching

Authentication was performed by entering a value of section containing the last spot of each stroke into the database first and comparing it with the same value that was calculated for the input signature. Here, spatial pyramid matching was used additionally to create a pyramid distinguishing the coordinate of the last spot on a space and gradually segmentalizing the space to compare and analyze the similarity level.

4.5. Boundary Matching

Boundary matching is a method that draws several lines on a signature input window and determines the order and number of strokes crossing the lines for comparison purposes. This method recognizes the separate input signatures as the same signature if the strokes cross the lines in the same order, even if their shapes show a little difference. For example, draw three equally spaced base lines (boundaries) on an input window before receiving a signature. Subsequently, each time the stroke crosses these lines, store the number assigned to each line in order, and then designate the stored combination of boundary numbers as the signature's own password. Subsequently, divide the password once again following the direction of the crossing stroke (up or down) and compare with other signatures. This is to minimize the margin of error occurring between the signatures, depending on the signer's mood or other conditions. These cause the password to move a section or several sections behind. Therefore, to remove any margin of error, compare the first and last sections to remove the section(s) of incorrect direction and make the database-stored section number identical with the section number of signature; finally, make a comparison after filtering the password value.

4.5.1. Dynamic Time Warping (DTW)

Often used for the pattern analysis of time series signals, the DTW algorithm is also being studied as a method of classifying signatures. One of the special advantages of the proposed system is that, when compared to the existing systems [4,5], a DTW and several other algorithms have been applied in combination with a variety of methods to instantly and intelligently recognize the authenticity of a signature to prevent any unauthorized signing by a third party. Here, the signatures were compared by calculating the global distance between two signatures after computing the velocity vectors for both X-axis and Y-axis by using the coordinate values that were obtained at the same time intervals and preprocessing the data that are necessary for the DTW algorithm-based calculations.

4.5.2. Basic DTW Algorithm

When there are two signatures Sa and Sb with respective length of n and m, $D(i,j)$ is a minimum distance between the i-th spot to the j-th spot of Sa and Sb, so that the overall minimum distance is $D(n,m)$. The equation is as follows:

$$D(i,j) = D(i-1,j-1) + mind(i-1,j), d(i,j-1), d(i-1,j-1) \tag{1}$$

where $d(i,j)$ represents the distance between the i-th spot and j-th spot of Sb.

$$d(i,j) = \left| \sqrt{x_i^2 + y_i^2} - \sqrt{x_j^2 + y_j^2} \right| \tag{2}$$

4.5.3. Improved DTW Algorithm

In this improved DTW algorithm, a method that integrates the distance vector with the angular distance has been proposed. By applying the distance to the earlier equation of the DTW algorithm (2), the following modification has been made:

$$d(i,j) = \alpha \times d_{length}(i,j) + \beta \times d_{<}(i,j) \tag{3}$$

where the values α and β are 0.4 and 0.6, respectively, and $d_{<}(i,j)$ and $d_{length}(i,j)$ are the respective distances against speed and angle. This can be calculated as:

$$d_{length}(i,j) = \left| \sqrt{x_i^2 + y_i^2} - \sqrt{x_j^2 + y_j^2} \right| \tag{4}$$

$$d_{<}(i,j) = 1 - \cos\theta \tag{5}$$

$$\cos\theta = \frac{\left(x_i^2 + y_i^2\right) + \left(x_j^2 + y_j^2\right) - \left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2}{\sqrt[2]{x_i^2 + y_i^2}\sqrt{x_j^2 + y_j^2}} \tag{6}$$

4.5.4. Method of Comparison

Calculate an adaptive threshold by using the maximum distance of inner class and standard deviation of the reference signature after composing five reference signatures to authenticate the signature:

$$maxIntraDist = \max_{i,j,i \neq j} D\left(S_i, S_j\right) \tag{7}$$

where maxIntraDist is the maximum distance of inner class and σ is the standard deviation of the same class. Thus, the adaptive threshold can be calculated as:

$$Threshold_{adaptve} = maxIntraDist + \sigma \times \tau \tag{8}$$

where parameter is $\tau = 0.1$.

The authenticity of a received signature will be proven by comparing each signature's average value of maximum distances and minimum distances and an adaptive threshold that is similar to five other signatures.

$$Dist(S_T, S_i) = \frac{maxD(S_T, S_i) + minD\left(S_T, S_j\right)}{2} \tag{9}$$

where S_T refers to the signature to be authenticated and S_i is the i-th signature among the five reference signatures.

If $Dist(S_T, S_i) \leq Threshold_{adaptive}$, the received signature is considered to be identical; If $Dist(S_T, S_i) > Threshold_{adaptive}$, it is not.

4.6. Hidden Markov Model Technique

The Hidden Markov Model (HMM) has modeled the generation process of the characteristics contained in a signal and it is widely used for voice recognition or gesture systems, since it provides a good recognition rate with little computational work [29]. HMM is divided into the learning process and recognition process. In the former, the feature points of an input pattern are represented with the state transition probability distribution, and the process having the probability distribution, wherein a specific symbol could appear in a certain state as a Markov process is assumed. These probability distributions are estimated with learning data.

The probability of revealing the input pattern in that model is calculated and recognized based on this estimated probability distribution. As observed in the process above, under the assumption that there is a state in a certain observable process, HMM computes the state transition probability wherein a new situation becomes dependent on the situation right before as well as the observation probability wherein the observed symbols (i.e., symbols that underwent transition) become dependent on the present state. HMM consists of three elements: the number of states, the state transition probability distribution that determines the changes in the state over time, and the probability distribution for output symbols in each state. Although individual states cannot be directly observed, it is possible to estimate the original state by observing the symbols that have been produced by each state with a certain probability. With such definitions, HMM can be represented as λ = (A, B, Π). Here, Π = π ij is the early-state transition probability distribution, A = a ij is the state transition probability distribution, and B = b ij is the observation-symbol probability distribution. The next two steps must be taken to use HMM. These are the process of model formation and the process of calculating the probability value of the observed symbol using an already formed model.

- Step 1: Model formation process a problem of computing model parameter λ = (A, B, Π) that has maximized P (O|λ).
- Step 2: Model recognition process computing the symbol's likelihood P (O|λ) for a model when both sequence T (O = O, 1⋯O, 2⋯O, for the symbol observed) and model λ = (A, B, Π) have been given.

4.7. Linear Discriminant Analysis

Linear discriminant analysis is one of the methods that finds optimal projection for classification. This technique involves finding a projection matrix that has the maximum proportion between the matrix that represents the distribution within a class and the matrix representing the distribution between the classes. Generally, when attempting to make a classification using this technique, one needs to project the input signature onto the low-level space using the principal component analysis technique to make the matrix representing the distribution within the class nonsingular prior to computing the optimal projection matrix. First, obtain the signature's X and Y coordinates, relevant time data, and acquire the input value with the following equation:

$$S_i = \left|x_1, y_1, t_1, x_2, y_2, t_2, \cdots, x_1, y_1, t_1\right|^T \tag{10}$$

Here x_1, y_1 refers to the coordinates of online-input signature at the time of t_1. The average vector of the signature used for the learning process can be represented as:

$$m = \frac{1}{P}\sum_{i-1}^{P} S_i \tag{11}$$

The following equation will be created by calculating the first dimensional vector for the learning signature that was used in this equation:

$$\overline{S} = \overline{S_1} \vdots \overline{S_2} \vdots \ldots \vdots \overline{S_P} \tag{12}$$

$$\overline{S_i} = S_i - m \tag{13}$$

Covariance matrix Ω for $\overline{S}$ made up with the N X P Equation (12) is identical with Equation (14), and its eigenvalue and eigenvector can be computed while using Equation (15).

$$\Omega = \overline{S}\overline{S^T} \tag{14}$$

$$\overline{S}\overline{S^T}v_j = \lambda u_j \tag{15}$$

Below is the equation for calculating an eigenvector for the learning signal x_i by using eigenvector v_i that was obtained with Equation (15). In other words, the feature vector of an input signal can be obtained by projecting the covariance eigenvector onto the space transformed by principal component analysis.

$$z_i = v_i^T(S_i - m) \tag{16}$$

If size $N \times N$ of covariance matrix Ω is large, one can calculate the eigenvector of the covariance matrix efficiently using the snap-shot method.

Meanwhile, linear discriminant analysis is a technique that performs linear transformation by using a matrix where the proportion between S_w (the matrix representing variance within the class) and S_B (the matrix representing the variance between classes) is maximized. The relevant equations are:

$$S_B = \sum_{i-1}^{c} n_i(m_i - m)(m_i - m)^T \tag{17}$$

$$S_B = \sum_{i-1}^{c} \sum_{s \in C_i} (S - m_i)(S - m_i)^T \tag{18}$$

In the equations above, N_i is the number of data in i-th class C_i, and m is the average of all data. In addition, M_i is the average of data transformed by the principal component analysis in class C_i. As shown in Equation (19), optimal projection matrix W is selected as a matrix with orthogonal rows and that maximizes the proportion between matrix S_W and S_B.

$$W = argmax_W \frac{\left|W^T S_B W\right|}{\left|W^T S_W W\right|} = [w_1, w_2, \ldots, w_m] \tag{19}$$

Here, as with Equation (20), w_i is a set of generalized eigenvectors for both S_B and S_W.

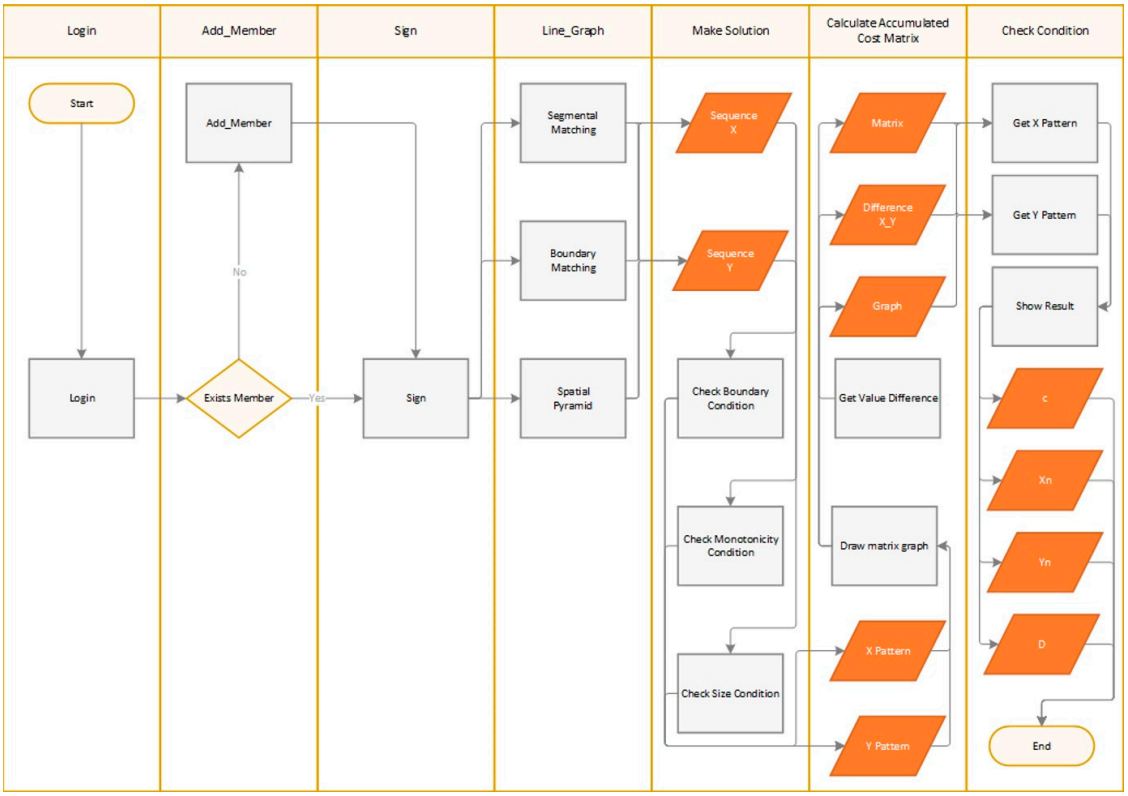
$$S_B w_i = \lambda_i S_W w_i, i = 1, 2, \ldots, m \tag{20}$$

$F = F_1, F_2, \ldots, F_N$ of input signature S_i can be obtained with Equation (21).

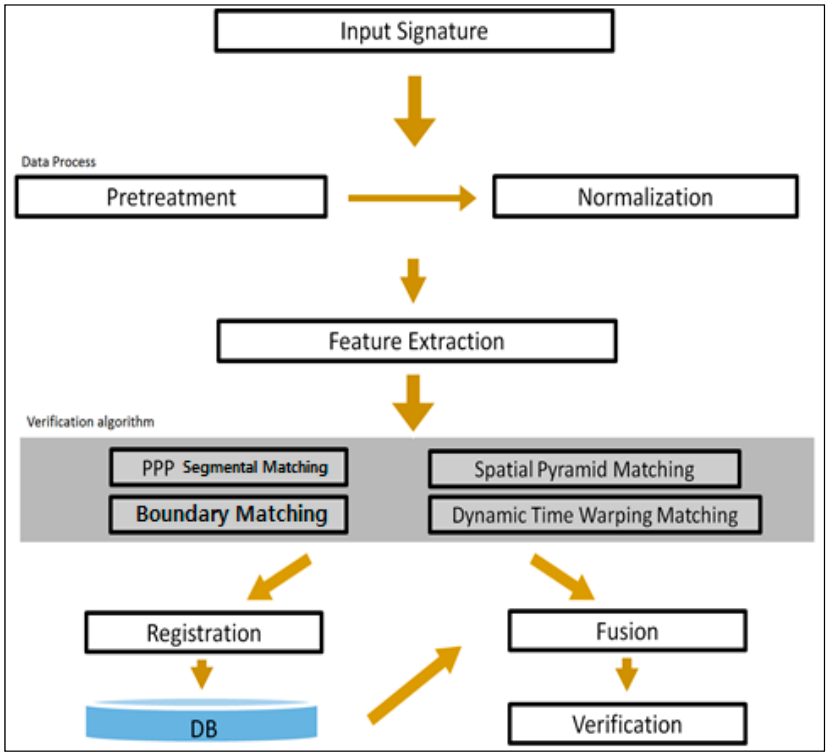
$$F_i = W^T z_i = W^T v_i^T (S_i - m) \tag{21}$$

5. System Implementation and Considerations

Figure 4 shows the overall system configuration, where the user signature will be entered first followed by its coordinates through a smart phone application. The coordinates of the received signatures are subjected to sampling based on the time spent writing the signatures and generalized by matching the sizes.



(**a**) System Mechanism.



(**b**) System Configuration.

Figure 4. Overall system configuration.

Next, the generalized coordinates are extracted to be transformed into forms that can be used for individual algorithms. The algorithms used for the implemented system include Partitioning Peak Points (PPP)/Segmental Matching, Boundary Matching, and DTW Matching Algorithms; others have been excluded, since they require complex arithmetic operations and do not serve the purpose of this paper. In each algorithm, the feature values between the signatures are calculated with the equation or method. The resulting values of the baseline signature will then be stored in the database to compare with other values for authentication.

Figure 5 shows the entire Java Android Unified Modeling Language (UML). (1) Add_member class is a class that shows the operation of adding the user to the database; it refers to the class that deals with the SQLite managing the database. (2) Login class performs the process of proceeding to the next step when the user inputs the ID stored in the database. (3) Sign class literally shows the user's signing process on a display, refers to the DataBase (DB) class, and delivers feature values to the database. (4) Line_graph class represents the database-stored values and analytical values with graphs following the standards. Histograms and pie graphs are common. (5) DB class deals with the database of an application. (6) Total_result shows the total average value of all the values analyzed before. (7) Display the analytical values related to partitioning, spatial pyramid, and boundaries on a display.

(1) Add_member class
(2) Login class
(3) Sign class
(4) Line_graph class
(5) DB class deals with the database of an application.
(6) Total_result shows the total average value of all the values analyzed before.
(7) Display the analytical values related to partitioning, spatial pyramid, and boundaries on a display.

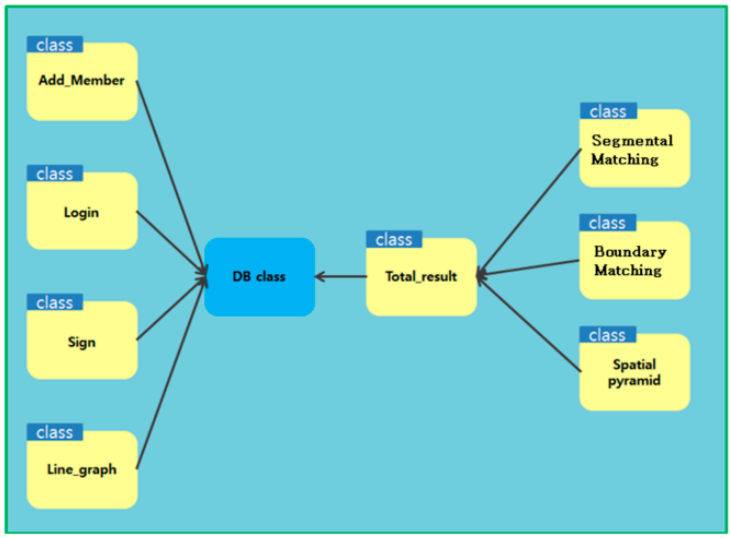


Figure 5. Entire unified modeling language.

In this study, a Java-based UML was developed based on several algorithms for the proposed surgery agreement signature authentication system. The operating mechanism is initiated by entering a sequence set for both X and Y, respectively, along with a time variable in Main Activity. The information necessary for DTW should be entered first and at this time the DTW algorithm is required to satisfy the conditions of pattern matching, so that it is necessary to confirm that whether the three elements satisfy the conditions at the check condition class. The necessary terms should be entered as variable and the functions in the class include the Endpoint Limit Condition Test, Monotonic Increase Limit Condition Test, and Step Increase Condition Test. When the conditions have been met, the process moves on to the 'make solution' class. A function that calculates the distance of each x-y grid is included in this class, where another function that outputs the distance values with a matrix-form graph is also included. Finally, the process moves on to the class where an accumulated cost matrix is computed based on the cost matrixes. By calculating some lowest possible matrix by accumulating the values, the minimum distance between X and Y patterns can be found with the intelligent agent implemented in the previous study for authentication. Figure 6 shows the UML of the surgery agreement signature authentication system.

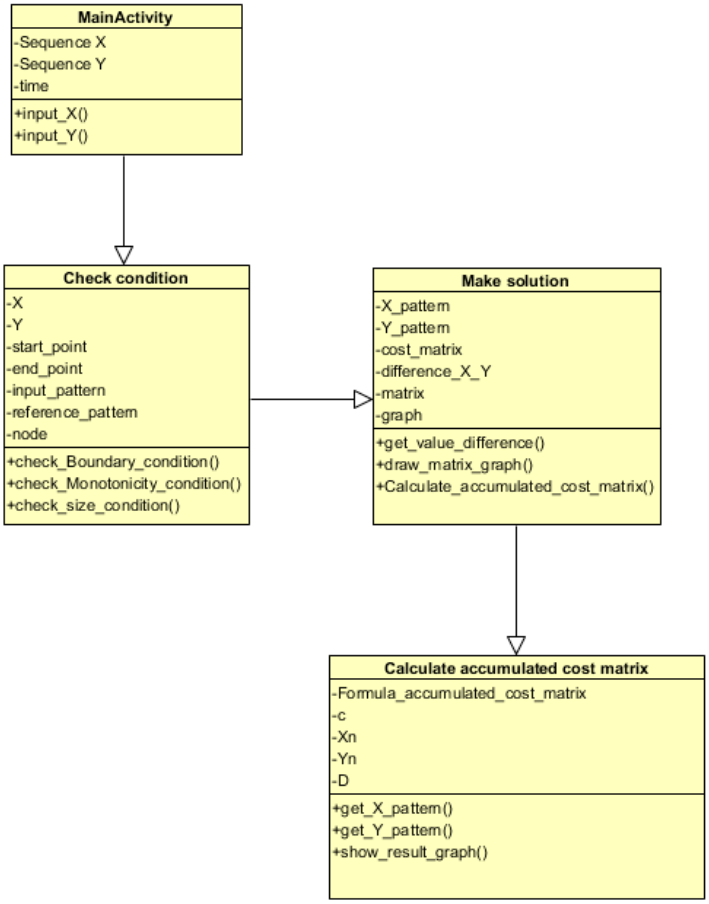


Figure 6. The UML of the surgery agreement signature authentication system.

Figure 7 is a login screen that will store the baseline signature of the user under his/her ID to compare it with other signatures received in the future. During the registration process, the ID of the user and the analytical values of his/her signature will be stored in the application database. In addition, the picture of the baseline signature will be stored in the memory storage of the smart phone or tablet as an image file.

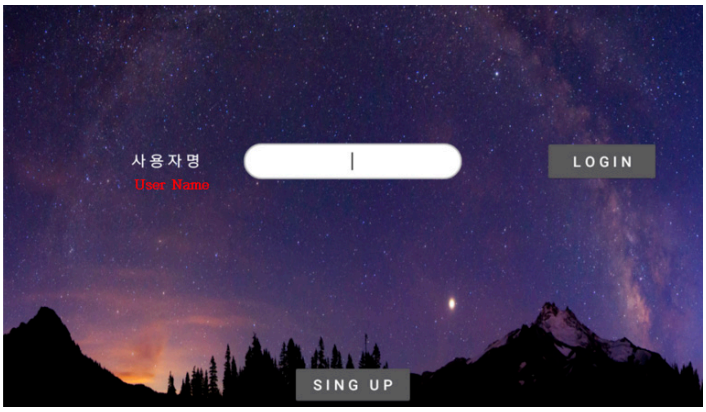


Figure 7. Login screen.

Figure 8 shows the signature to be entered for comparison. The analytical values are extracted in order to compare them with the DB-stored baseline signature. Similar to the baseline signature, this is stored in the database as an image file.

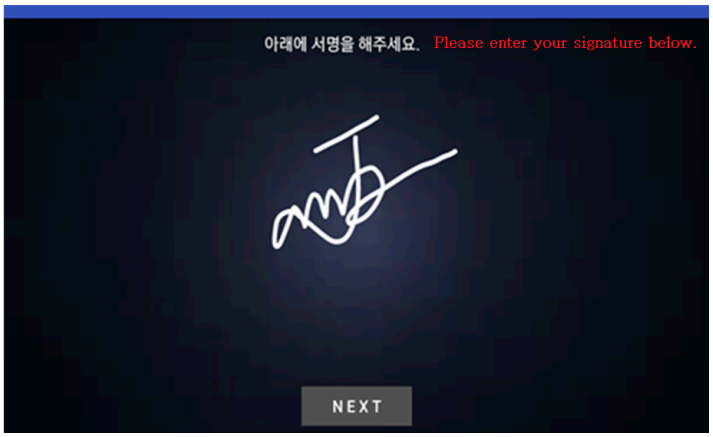
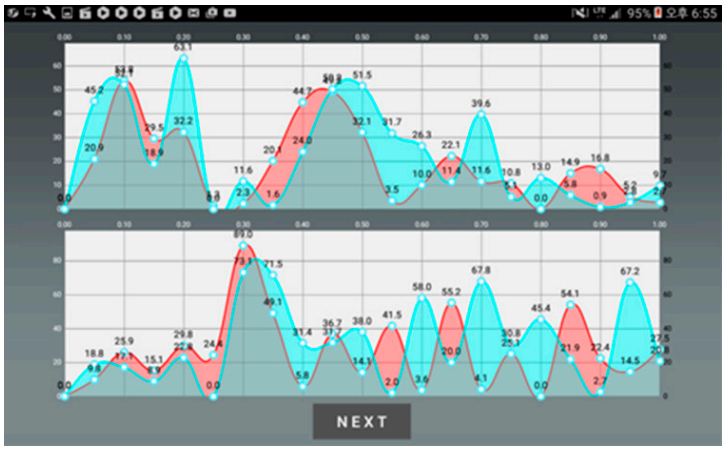
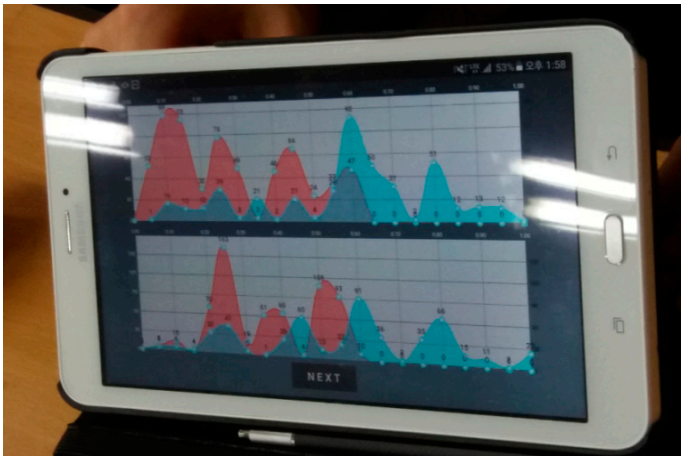


Figure 8. Signature input window for comparison.

Figure 9 shows the displacements of both the baseline signature and the comparison signature over time with graphs. The graph above represents the X-displacements, whereas the graph below shows the Y-displacements. The light green areas indicate the DB-stored signature and the red parts represent the signature subject to comparisons.



(**a**) A design of signature displacement comparison graph.



(**b**) A test bed of signature displacement comparison graph.

Figure 9. Design and test bed of Signature displacement comparison graph.

Figure 10 shows the image files of both signatures that are mentioned above and indicates the final comprehensive matching rate with a pie graph. The comprehensive matching rate was calculated by taking the averages in each algorithm. After setting the optimal probability boundary suitable for each algorithm, the system checks the analytical values as to whether they exceed the boundaries or if the average value exceeds the threshold. In either case, the signatures are deemed to be identical if the values exceed the boundary or threshold.

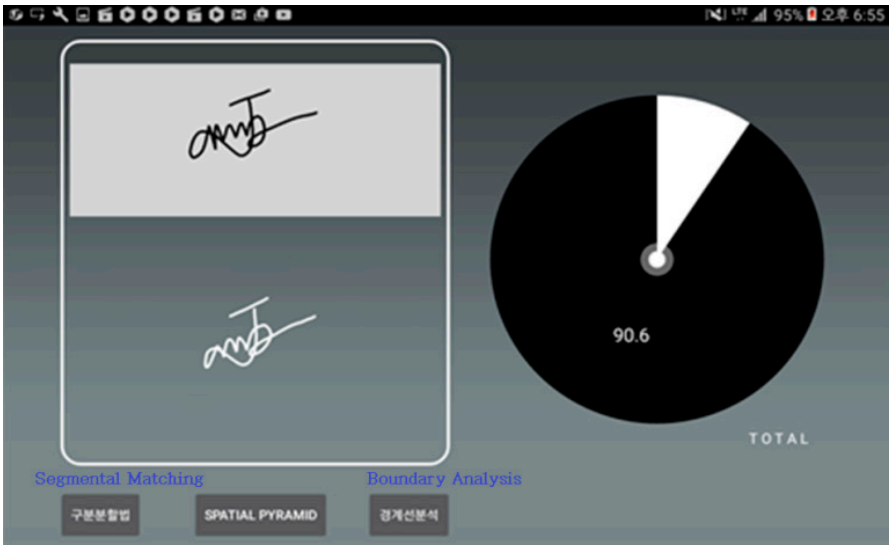


Figure 10. Final comparison screen.

Figure 11 shows the matching rate calculated with the segmental matching method. The graph on the left shows the comparison result of the times when the peaks were generated, and the right graph indicates the matching rate based on the number of peaks in each section.

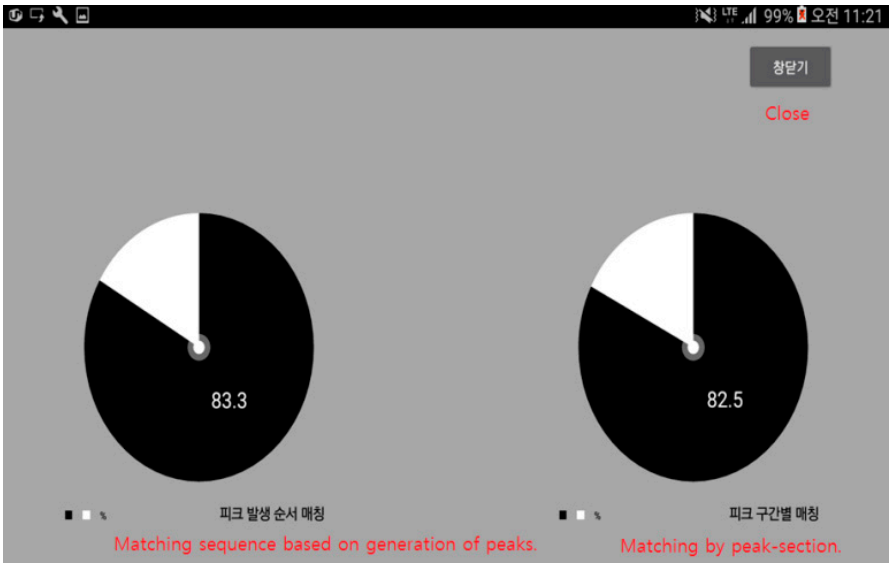


Figure 11. Result of segmental matching.

Figure 12 shows the matching rate after performing spatial pyramid matching. The graph on the left is the resulting rate after applying the spatial pyramid matching algorithm, and the one on the right shows the results that were obtained by comparing the spots where the strokes end.

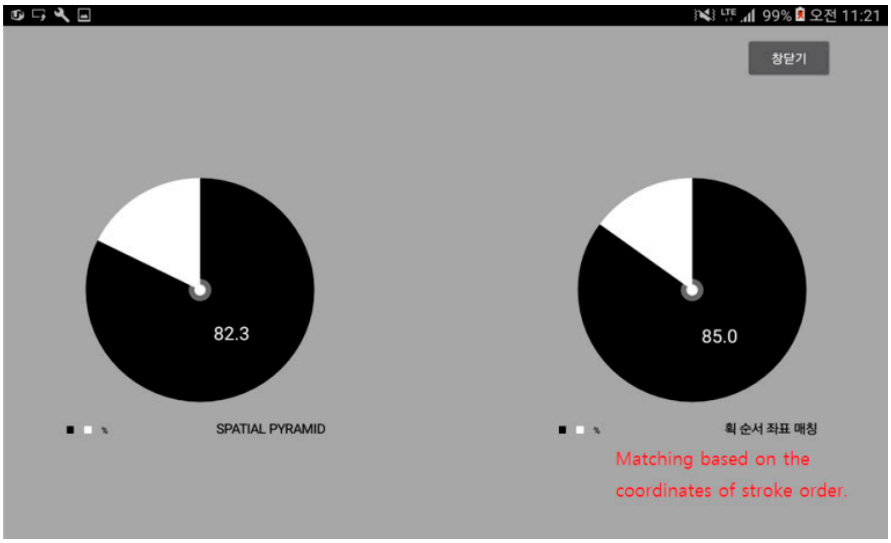


Figure 12. Result of Spatial Pyramid Matching.

Finally, Figure 13 shows the resulting matching rate after performing boundary matching. The left graph shows how much the analytical values contributed to the matching result, whereas the values in the upper right are the analytical values of boundaries that were stored in the Database (DB). The lower values are for the boundaries of input signature. Comparisons of these values have been performed for each section.

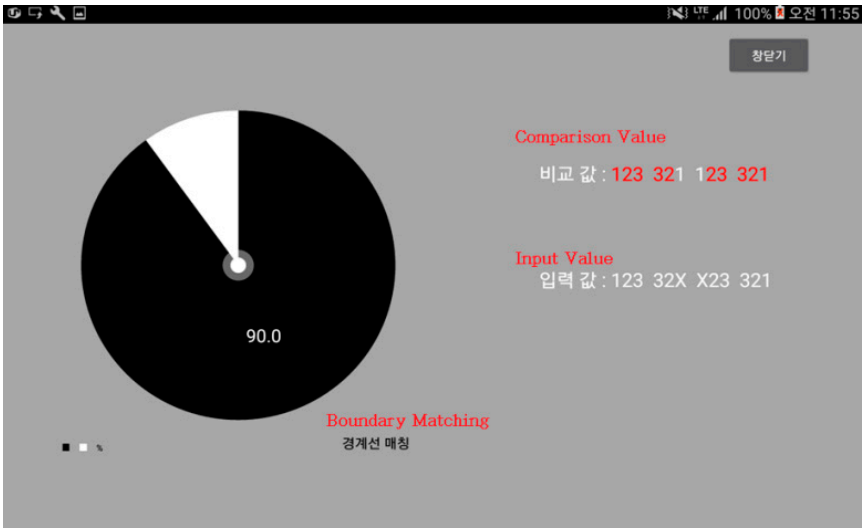


Figure 13. Result of Boundary Matching.

After receiving the same signatures five times from about 200 people (approx. 1000 signatures), the resulting values were confirmed to be different between the people while using their names as their signatures and the people who use their own (other than names) signatures. While the result of segmental matching showed similar higher matching rates for both groups, the result of spatial pyramid matching revealed that those who use their names exhibited higher precision. Contrary to this result, the same people showed lower precision when boundary matching was used. For the people who have their own special signatures, the precision level was higher when boundary matching was applied.

The proposed system includes such a function, so that the customer's signature is compared with the card holder's actual signature information registered in advance and the relevant parties, including

the card holder himself/herself, will be notified of the analysis result. The details of this technology have been proposed to "H" hospital in Republic of Korea as a prototype.

6. Discussion

Until recently, hospital patients or their guardians were required to sign a surgery consent form one by one to receive a surgical procedure, but hospitals are now attempting to digitalize such a process to prevent its loss or delayed confirmation. Additionally, as this consent form becomes an important legal evidence for proving when the signature was entered, such an effort is necessary in the occasional cases when the signature was entered after the procedure.

Thus, a surgery consent (agreement) signature authentication system has been proposed in this paper specifically for the mobile health care field. The proposed electronic system can replace all of the paper forms used at the hospitals, including surgery/private information collection agreement forms. The electronic forms can be checked and signed on a smart phone or tablet Personal Computer (PC) used by the hospital and, since they are quite similar to a paper form, the signature will be accepted even if it deviates from the input window. They are then delivered to the operating room immediately after being authenticated, so that the possibility of loss/misplacement/delay will be avoided. It is not necessary to scan these forms and those patients with mobility difficulties can receive explanations while checking them on a tablet PC directly.

One of the special advantages of the proposed system is that, when compared to the existing systems [4,5] its signature authentication algorithm is able to recognize the signature instantly and intelligently determines whether it has been entered by the patient in person, preventing the possibility of unauthorized signing by a third party. Additionally, the system does not allow the time of signing to be altered in any way that it can be used for digital forensics. In the paper, an effort was made to improve the vulnerabilities of the existing systems and the compatibility test obtained a successful result.

7. Conclusions

Requiring the hospital patients or their legal guardians to sign a paper surgery or personal information collection consent form has been a common practice until recently. However, hospitals are trying to upgrade such a process through digitalization, due to the administrative inefficiencies involved (e.g., its loss or delayed delivery/notification). This study focuses on developing a digital signature authentication system for the use in the field of mobile heath care.

This research was used for implementing an improved DTW algorithm, where a basic DTW and the signing speed characteristic are used along with the distance measuring method that considers the angular variations. Additionally, instead of using each algorithm separately for signature analysis, all of the algorithms were used to perform analysis across several stages. An intelligent agent provides assistance during the analysis process. It was recognized that the accuracy of the analysis was much better when all the algorithm were used together. Additionally, the recognition rate of each algorithm was different, depending on the signature form. Thus, a system where the cloud database intelligently selects an algorithm with the help of an intelligent agent for the efficiency of the entire system has been designed and implemented.

The test bed experiment result showed that the system was flexible and efficient. Thus, in this paper, signatures were analyzed while using segmental, spatial pyramid, and boundary matching techniques instead of the existing popular DTW Algorithm. Likewise, instead of analyzing the signatures with the respective algorithm, all of the discussed algorithms were used in several stages. As a result, the precision level was higher than the one obtained from a single-algorithm analysis, which meant that the recognition rates would vary, depending on the form of the signature and the algorithm used.

The electronic consent form proposed in this paper can replace all of the paper documents (e.g., surgery consent forms, Agreement on Offering Personal Information, etc.) used at the hospitals and be checked and signed on a smart phone or tablet PC. It is similar to actual paper forms, as the

signature can be entered, even if it extends beyond the boundary of the input window. The consent form is then sent to the operating room as soon as it is completed, so that both the patient and hospital do not have to worry about losing it or scanning it separately. The mobility-impaired patients can receive explanations just by watching them on a tablet PC and fill out the consent form on the spot. All of the data collected will be managed safely by the hospital information system. This paper conducted a signature analysis using segment division matching, spatial pyramid matching and boundary matching instead of the DTW algorithm, which is a widely known signature analysis method. Instead of analyzing signatures by using each algorithm one by one, this study uses multiple algorithms and analyzes the signatures in various steps. Through this, it was found that the application of various algorithms could enhance accuracy more than a signature analysis that uses only one algorithm. Additionally, the results showed that algorithms with good signature recognition may vary by the type of signature. Accordingly, cloud databases should be designed and implemented, so that algorithms intelligently select for efficient application.

One of the major demerits of this study was that the signatures were received by only using smart phones or Tablet PC (Personal Computer), and the analyses were based on their moving routes and speeds. More precise analyses could have been performed with more information obtainable through Electronic Pen Mouse or Exclusive Touch Pad. The author expects this technology to contribute to the field of biometric identification. The limit of this study is that the signature verification performance of the proposed system deteriorates when the signature is not entered by the actual cardholder, or when it is used at restaurants or pubs serving alcoholic beverages. This problem will be dealt with in the authors' future work. Additionally, in the future work, this system will be proposed to the Korean credit card companies or for the smart banking systems to strengthen the security during the transmission process to achieve the similar level of security as encryption.

Funding: This work was supported by the Korea Maritime and Ocean University Research Fund.

Conflicts of Interest: The author declares no conflict of interest.

Abbreviations

DWT	Discrete Wavelet Transform
CVC	Card Verification Code
DB	Database
DTW	Dynamic Time Warping
PCA	Principal Component Analysis
HMM	Hidden Markov Model
SVM	Support Vector Machine
PPP	Partitioning Peak Points
UML	Unified Modeling Language
PC	Personal Computer

References

1. Thuemmler, C.; Bai, C. *Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare*; Springer: Berlin, Germany, 2017; pp. 91–107.
2. Huh, J.-H.; Kim, T.-J. A location-based mobile health care facility search system for senior citizens. *J. Supercomput.* **2018**, *75*, 1831–1848. [CrossRef]
3. Ratha, N.K.; Connell, J.H.; Bolle, R.M. Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst. J.* **2001**, *40*, 614–634. [CrossRef]
4. FORCS Co., LTD. Available online: http://www.forcs.com/kr/ (accessed on 1 May 2020).
5. Bitcomputer. Available online: https://www.bit.kr/ (accessed on 1 May 2020).
6. Lu, C.-S.; Liao, H.-Y.M. Structural digital signature for image authentication. In Proceedings of the 2000 ACM workshops, San Antonio, TX, USA, 2–7 June 2000; pp. 115–118.

7. Chin, W.; Saw, S.H.; Yap, S.G. A Simple Interactive 3D Interior Design Application for Living Room—Cost Management. *J. Multimed. Inf. Syst.* **2017**, *4*, 157–162.
8. Somani, U.; Lakhani, K.; Mundra, M. Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In Proceedings of the International Conference on Parallel Distributed and Grid Computing (PDGC), Solan, India, 28–30 October 2010; pp. 211–216.
9. Merkle, R.C. A Certified Digital Signature. In Proceedings of the Conference on the Theory and Application of Cryptology, Santa Barbara, CA, USA, 20–24 August 1989; pp. 218–238.
10. Karimov, M.M.; Tashev, K.A.; Islomov, S.Z.u.; Mavlonov, O.N. Triangle Method for Fast Face Detection on the Wild. *J. Multimed. Inf. Syst.* **2018**, *5*, 15–20.
11. Maged Fahmy, M.M. Online handwritten signature verification system based on DWT features extraction and neural network classification. *Ain Shams Eng. J.* **2010**, *1*, 59–70. [CrossRef]
12. Madasu, V.K.; Lovell, B.C.; Kubik, K. Automatic handwritten signature verification system for australian passports. In Proceedings of the Science, Engineering and Technology Summit on Counter Terrorism Technology, Canberra, Australia, 14 July 2005; pp. 53–66.
13. Zimmer, A.; Ling, L.L. A hybrid on/off line handwritten signature verification system. In Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR'03), Edinburgh, UK, 3–6 August 2003; Volume 1, p. 424.
14. Trevathan, J.; Read, W.; McCabe, A. Neural Network-based Handwritten Signature Verification. *J. Comput.* **2008**, *3*, 9–22.
15. McCabe, A.; Trevathan, J. Markov Model-Based Handwritten Signature Verification. In Proceedings of the International Conference on Embedded and Ubiquitous Computing, IEEE, Shanghai, China, 17–20 December 2008; pp. 173–179.
16. Tolba, A.S. GloveSignature: A Virtual-Reality-Based System for Dynamic Signature Verification. *Digit. Signal Process.* **1999**, *9*, 241–266. [CrossRef]
17. Inan Majid, G.M. A different approach to off-line handwritten signature verification using the optimal dynamic time warping algorithm. *Digit. Signal Process.* **2008**, *18*, 940–950.
18. Bandyopadhyay, S.K.; Bhattacharyya, D.; Das, P. Handwritten signature recognition using departure of images from independence. In Proceedings of the 3rd IEEE Conference on Industrial Electronics and Applications (ICIEA 2008), IEEE, Singapore, 3–5 June 2008; pp. 964–969.
19. Zimmer, A.; Ling, L. Offline Signature Verification System Based on the Online Data. *EURASIP J. Adv. Signal Process.* **2008**, *112*. [CrossRef]
20. Alonso-Fernandez, F.; Fierrez, J.; Gilperez, A.; Galbally, J.; Ortega-Garcia, J. Robustness of signature verification systems to imitators with increasing skills. In Proceedings of the 2009 10th International Conference on Document Analysis and Recognition, Barcelona, Spain, 26–29 July 2009.
21. Garcia-Salicetti, S.; Houmani, N.; Dorizzi, B. A Novel Criterion for Writer Enrolment Based on a Time-Normalized Signature Sample Entropy Measure. *EURASIP J. Adv. Signal Process.* **2009**, *9*, 26–29. [CrossRef]
22. Lee, L.L.; Berger, T.; Aviczer, E. Reliable on-line human signature verification systems. *IEEE Trans. Pattern Anal. Mach. Intell.* **1996**, *18*, 643–647. [CrossRef]
23. Ong, T.S.; Khoh, W.H.; Teoh, A.B.J. Dynamic Handwritten Signature Verification Based on Statistical Quantization Mechanism. In Proceedings of the International conference on computer engineering and technology (ICCET'08), Singapore, 22–24 January 2009; Volume 2, pp. 312–316.
24. Nakanishi, I.; Sakamoto, H.; Nishiguchi, N.; Itoh, Y.; Fukui, Y. Multi-Matcher On-Line Signature Verification System in DWT Domain. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2006**, *89*, 178–185. [CrossRef]
25. Lejtman, D.Z.; George, S.E. On-line handwritten signature verification using wavelets and back-propagation neural networks. In Proceedings of the International Conference on Document Analysis and Recognition, IEEE, Seattle, WA, USA, 13 September 2001; pp. 992–996.
26. Nanni, L.; Lumini, A. A novel local on-line signature verification system. *Pattern Recognit. Lett.* **2008**, *29*, 559–568. [CrossRef]
27. Nakanishi, I.; Nishiguchi, N.; Itoh, Y.; Fukui, Y. On-line signature verification based on subband decomposition by DWT and adaptive signal processing. *Electron. Commun. Jpn.* **2005**, *88*, 1–11. [CrossRef]

28. Enqi, Z.; Jinxu, G.; Jianbin, Z.; Chan, M.; LinJuan, W. On-line Handwritten Signature Verification Based on Two Levels Back Propagation Neural Network. In Proceedings of the International Symposium on Intelligent Ubiquitous Computing and Education (IUCE), Sichuan, China, 15–16 May 2009.
29. Liu, K.; Nasser, K.; Matthias, C. Comparison of two real-time hand gesture recognition systems involving stereo cameras, depth camera, and inertial sensor. *SPIE Photonics Eur. Int. Soc. Opt. Photonics* **2014**. [CrossRef]
30. Govindarajan, M.; Chandrasekaran, R.M. Online signature verification using bagged svm classifier. *Asian J. Comput. Sci. Inf. Technol.* **2013**, *1*, 71–74.
31. Huh, J.-H. *Smart Grid Test Bed Using OPNET and Power Line Communication*; IGI Global: Hershey, PA, USA, 2018; pp. 1–425.
32. Lee, D.J.; Go, H.J.; Chun, M.-G. Signature Verification using Segment Matching and LDA Method. *KIISE* **2007**, *34*, 1065–1074.
33. Lazebnik, S.; Schmid, C.; Ponce, J. Beyond Bags of Features: Spatial Pyramid Matching for Recognizing Natural Scene Categories. In Proceedings of the IEEE Conference Computer Vision and Pattern Recognition, New York, NY, USA, 17–22 June 2006; Volume 2, pp. 2169–2178.