Handwritten Digital Signature Accuracy Enhancement Comparison on Android Based Mobile Application System

S Rohajawati*[1], A Ismail[2], I P Gunawan[3], B A Sitorus[4]

[1,2] Department of Information Systems, Universitas Bakrie

[3] Department of Informatics, Universitas Bakrie

[4] Data Science, Faculty of Science, Universiteit Leiden

E-mail: siti.rohajawati@bakrie.ac.id[1], 1152002006@student.bakrie.ac.id[2], irwan.gunawan@bakrie.ac.id[3] , brian.arnesto.sitorus@umail.leidenuniv.nl[4]

Abstract: The research reported in this paper aimed to improve the quality size ratio and storage size of digital signature used in the e-form Fumida app, a mobile application employed by PT Fumida Pestindo Jaya for pest control, termite control, and fumigation services for data collection and verification. The application was developed using the Mobile Application Development Life Cycle (MADLC) method and utilized as a replacement for paper media used to fill in data related to work with the digital signature feature from which verification/authentication of the work results carried out by Fumida to its clients is given. While replacing paper forms, the original digital signature suffered quality and accuracy loss when resized for printing, prompting the investigation of three methods to enhance their integrity. This process was subsequently examined using a questionnaire with the help of 22 respondents and calculation of questionnaire data. The results of our study showed that our model 3 emerged as the most effective solution, maintaining high image quality and accuracy even when resized.

Keywords: digital signature; Android; Mobile Application Development Life Cycle (MADLC)

1. Introduction

The COVID-19 pandemic in Indonesia has accelerated the adoption of digital signatures, particularly for document approvals [1]. Digital signature serve as a virtual equivalent to handwritten signatures or seals[2], offering the added benefit of enhanced security. Unlike their physical counterparts, DS can validate the authenticity and integrity of messages, software, and virtual documents, providing a more secure and reliable way to conduct business electronically. PT Fumida Pestindo Jaya (Fumida) is a company that provides pest control, termite control, and fumigation services. Currently, Fumida is implementing technology in its business processes, including the use of an Android-based e-form Fumida application. This application replaces paper media that was originally used as form when the Fumida sales team or technical team performs its work. The e-form Fumida mobile application has several advantages over traditional paper forms [3], [4]. First, it is more efficient and convenient. The application can be accessed and filled out on any mobile device, which makes it easier for the sales and technical teams to work from anywhere. Second, the application is more secure [5], [6]. The signatures and data entered into the application are encrypted, which helps to protect them from unauthorized access [7]. Third, the application is more environmentally friendly [8], [9], [10] as it removes the requirement for paper, thereby minimizing waste.

Currently, the initial business process before filling out the Fumida e-form is as follows:

- Prospective customers will contact Fumida's call centre numbers or via email to consult and/or negotiate with prospective customers for the pest control, termite control, and/or fumigation process. Prospective customers can be individuals or companies.
- However, before work (treatment) can be carried out, a survey must first be conducted at the location where the work will be carried out to ensure what handling needs to be done further in the future (survey object). Survey objects can be private homes, offices, food/non-food factories, and so on.
- In the survey process, the Fumida sales team is the party that acts as the surveyor. The Fumida technical team is the party that acts as the executor in the treatment (treatment) of pest control, termite control, and/or fumigation.
- The e-form is divided into two categories, namely, the survey results e-form and the work report e-form. The e-form contains important data and information for further processing by the Fumida back-office team and is validated by the presence of electronic/digital signature (hereinafter referred to as "digital signatures"). The signature is done by the Fumida party (sales team/technical team) and the customer who has been surveyed and/or worked on. This is done to ensure that the data entered by the Fumida party is accurate and known by the customer.

The accuracy and size of data stored on the Android device are important factors for the Fumida e-form application. This is because the data entered into the application is used to generate reports and invoices for customers. The accuracy of the data is important to ensure that the reports and invoices are accurate and complete. The size of the data is also important to ensure that the application runs smoothly and does not take up too much storage space on the device. Subsequently, the signature process must also be able to provide a level of accuracy and size, both in terms of the length/width ratio of the image generated after the signature is performed or in the storage size of the image. The digital signature must have a consistent size with the manual signature to ensure that it is valid.

Traditionally, the accuracy and size of digital signatures in the Fumida e-form application can be compared with manual and digital signatures. The analysis should take into account the following factors:

- Ratio: The ratio of the length to width of the image generated after the signature is performed.
- Storage size: The size of the image generated after the signature is performed.
- Image quality: The clarity and sharpness of the image generated after the signature is performed.

Currently, two images of the Fumida e-form processing results in the form of digital signatures from the process that have been carried out in Portable Network Graphics (PNG) format are stored for comparison with manual signatures. A problem was identified in the digital signature of the Fumida e-form application, where all of the signature results looked blurry and displayed incomplete signature lines (dotted) after the form data was converted to PDF format by the system. This is a problem that needs to be alleviated because the signature will become inaccurate due to the blurred and incomplete image. On the contrary, in the manual signature model, there should be a minimum chance of a blurry or dotted signature. However, such distortions may still occur if the signing medium is problematic; e.g., the ink pen is (near) empty, paper is too slippery, etc. There are some possible causes of the problem that has surrounded the degraded quality of digital signature used in Fumida application; it may be due to the a low-quality camera or sensor to capture the signatures during the acquisition process, followed by an overly aggressive compression algorithm, as well as the use of sub-optimal rendering algorithm for signature images.

Based on the abovementioned problems, the research conducted in this current paper can be formulated as follows. Firstly, our research is concerned with converting a manual signature to a digital signature in the mobile application settings. This problem aims to develop a method that can accurately and reliably convert manual signatures into digital signatures that can be used in the Fumida e-form application. Secondly, our research is concerned with the comparison of digital signature to manual signatures. This problem aims to develop a method that can accurately and reliably compare digital signature to manual signatures. This method can be used to verify the authenticity of digital signature and to ensure that they are valid as required by the Fumida business process.

This paper is divided into several sections. First, a survey of the literature surrounding the state-of-the-art use of digital signatures will be explained. Second, the development of the Android-based application used in the research will also be presented. Third, the data collection methods that support the research will be described. Next, the results of data collection in the research will be elaborated in detail, so that the conclusions of this research can be obtained.

2. Literature Review

2.1. Handwritten Digital signature

Digital signature is the digital equivalent of a handwritten signature or stamped seal, with more inherent security features such as authentication and integrity. Hand-written digital signature refers to a specific type of electronic signature where people draw their signature on a touch screen or touchpad. Alternatively, it could also refer to digitization of physical handwritten signature (on paper) that subsequently used to associate it with document electronically [11]. Visually, handwritten digital signature may offer some resemblance to the physical signature although it does not provide the same level of security as a true digital signature, where some encryption methods might be applied.

The significance of digital signatures spans various fields such as security, document integrity, and efficiency. Previous studies have emphasized the importance of digital signatures in enhancing security and ensuring document integrity. For example, digital signatures provide robust authentication mechanisms that verify the identity of the signer and ensure the data has not been altered [12]. Additionally, digital signatures streamline business processes, reducing the time and cost associated with paper-based signatures[2]. Studies have shown that the adoption of digital signatures can lead to significant improvements in operational efficiency and data security [13].

Research reported in [1] investigated what motivates consumers to adopt digital signature technology, drawing upon three leading behavioural frameworks: (i) the unified theory of acceptance and use of technology (UTAUT), (ii) the theory of planned behaviour, and (iii) the information acceptance model. Ultimately, the authors in [1] found that consumer attitudes towards digital signature strongly influenced their willingness to use them. This underlines the importance of fostering positive perceptions about the technology’s benefits and security to ensure its sustainable adoption. The study’s finding that positive consumer attitudes strongly influence adoption underlines the critical role of addressing user perceptions and concerns. Focusing on building trust and confidence in the signature system’s security and benefits will be crucial for ensuring its long-term success.

Handwritten signature image is reported in [14] to be invariant with respect to several conditions such as changes in colour, orientation on paper, line thickness and dimensions. Hence, it can be used to perform off-line signature verification procedure. The invariance of handwritten signature image can then be described digitally based on a normalized image of the signature and digitized in the visible range of the electromagnetic spectrum. The digital description utilizes calculation of the distribution of its local features.

Handwritten digital signature has lend itself to the situation where mobile device is used, especially with the proliferation of mobile device nowadays. The performance of the use of digital signature (digital signatures) using mobile devices was investigated in [15], where five different devices was analyzed. The study experimented on the digital signature process using online method. The online signature method is usually done on specialized devices, such as using a digital pen tablet. The authors in [15]onducted tests to see if the digital signature process could be successfully applied with portable devices with different sizes and screen technologies (capacitive and resistive). Based on their results, it was found that the digital signature process (digital signature) with the online method can be fully implemented on portable devices by developing two different algorithms. These two algorithms are used to produce results that can be compared to each other and help improve the process's accuracy and reliability.

Relevant theories supporting the need for improved digital signatures include cryptography and information security. Cryptography provides the foundational technology that enables the creation and verification of digital signatures. Cryptographic algorithms ensure that digital signatures are secure and tamper-proof, making them essential for protecting sensitive information [16]. Information security theories also emphasize the importance of digital signatures in maintaining data confidentiality, integrity, and availability. By ensuring that only authorized individuals can sign documents and that the contents of the documents remain unchanged, digital signatures contribute significantly to overall information security [17].

Comparative analysis of handwritten signature and digital signature, in addition to cutting-edge biometric approach is reported in [11]. It explored their distinct traits, analysed their strengths and weaknesses, and even created models based on their technical features to understand their value. These models are derived from calculating potential profits from using different cryptographic and authentication methods in each signing approach. Subsequently, research reported in [18] proposed a method to verify the authenticity of handwritten signatures by combining two powerful tools: digital image processing and artificial neural networks (ANNs). Specifically, the ANNs use a technique called backpropagation learning to "train" themselves on real signatures and identify forgeries. This research has the potential to significantly improve the security of documents and transactions that rely on handwritten signatures. Furthermore, [19] tackles several problems that are challenging foauthentic or forgery signature verification by proposing a technique for offline signature verification (OSV), which aims to automatically distinguish genuine signatures from forgeries. Their proposed method analyzes unique characteristics of a signature, like pen movement, speed, and loop shape. The method merges information from two types of features: 22 Gray Level Co-occurrence Matrix (GLCM) features that capture texture information, and 8 geometric features that describe the signature's shape. This combined approach can select the most informative features for accurate verification, leading to more secure authentication processes and improving security for individuals, systems, and services.

2.2. Mobile Application Development Life Cycle (MADLC)

Mobile Application Development Life Cycle (MADLC): Mobile Application Development Life Cycle (MADLC) is one of the methods in the development of mobile-based applications [20]. Because mobile applications have complex functionality that is different from desktop applications, MADLC is proposed to allow a systematic approach to its development.

The Mobile Application Development Life Cycle (MADLC) is a systematic approach used in developing mobile applications. MADLC includes several phases: identification, design, development, prototyping, testing, and maintenance. This method is appropriate for the development of mobile-based applications due to its structured approach, which ensures that all aspects of the application are thoroughly tested and refined before deployment [21]. Compared to other methods, MADLC provides a comprehensive framework that addresses the unique challenges of mobile application development, such as varying device specifications and user interfaces. The MADLC method was chosen for this research because it allows for iterative testing and refinement, ensuring that the final application is both functional and user-friendly [22].

According to [23], MADLC has several phases in the process of developing mobile-based applications, including the following:

- Identification Phase: In this first phase, ideas are collected and categorized. The main goal is to come up with new ideas or improvements to existing applications.
- Design Phase: In this phase, the ideas of the mobile application team are developed into several application designs.
- Development Phase: In this phase, the application is coded.
- Prototyping Phase: In this phase, the functional requirements of each prototype are analyzed, tested, and sent to the client for feedback.
- Testing Phase: This phase is the most important. The prototype is tested on an emulator/simulator and also on a real device.
- Maintenance Phase: This phase is the last phase of the model and maintenance is an ongoing process. If errors/bugs are found, they can be fixed immediately, application security adjustments, function updates, interface updates on a regular basis, and other improvements.

MADLC phases can be illustrated as follows:

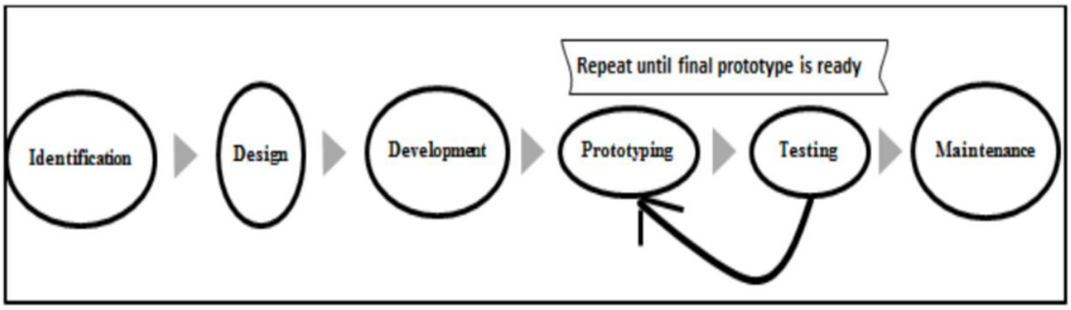


Figure 1. MADLC phases [23].

A recent approach in MADLC combines the method with the elements of computational thinking (CT), namely abstraction, algorithm, decomposition, pattern recognition and evaluation.

2.3. Literature Selection

The criteria for selecting the literature reviewed in this study included relevance to the topic, credibility of the sources, and the date of publication. Studies that provided empirical data on the effectiveness of digital signatures, discussed advancements in cryptographic techniques, or detailed the development processes for mobile applications were prioritized. Exclusion criteria included studies that were outdated or lacked peer review. This selection process ensured that the literature review was comprehensive and included only high-quality, relevant studies. Specifically, priority was given to research published in the last ten years to ensure the inclusion of the most recent advancements and findings in the field. Studies were also evaluated based on their methodological rigor, with preference given to those employing robust research designs and statistical analyses. Articles from reputable journals and conferences were given precedence to ensure the credibility and reliability of the sources.

To provide a comprehensive background for the research, a thorough review of relevant literature was conducted. This included a wide range of studies from various fields related to digital signatures, mobile application development, and cryptography. By reviewing a substantial amount of literature, the study ensured that it covered all necessary aspects and provided a solid foundation for the research. The diversity of sources, including journals, conference papers, and technical reports, contributed to a thorough and nuanced discussion of digital signatures and their application in mobile technology. The literature review process involved systematically searching for and evaluating studies that addressed the key themes and issues relevant to this research, ensuring a well-rounded understanding of the topic.

3. Research Method

The research method is depicted on Figure 2.

3.1. Literature Study.

It is conducted by searching and exploring knowledge, analyzing the analysis and design of Android mobile-based applications, the digital signature process and digital images [24], and comparing manual and DS. process as well as digital images; comparison of manual and DS. References were obtained from various sources, including scientific journals, e-books, papers, books, theses, projects, and so on.

3.2. Observation and Problem Identification

This step was conducted by visiting PT Fumida Pestindo Jaya to observe the use and functionality of their current e-form application. We focused on understanding the benefits, usability, and the existing digital signature process. The process followed the usability testing methodology Rubin & Chisnell (2008) described in “Handbook of Usability Testing.” This included developing a test plan, setting up a testing environment, preparing test materials, and conducting the test sessions. Problems are solved if the DS on the e-form is not appropriate or has a different level of similarity with manual signatures (paper).

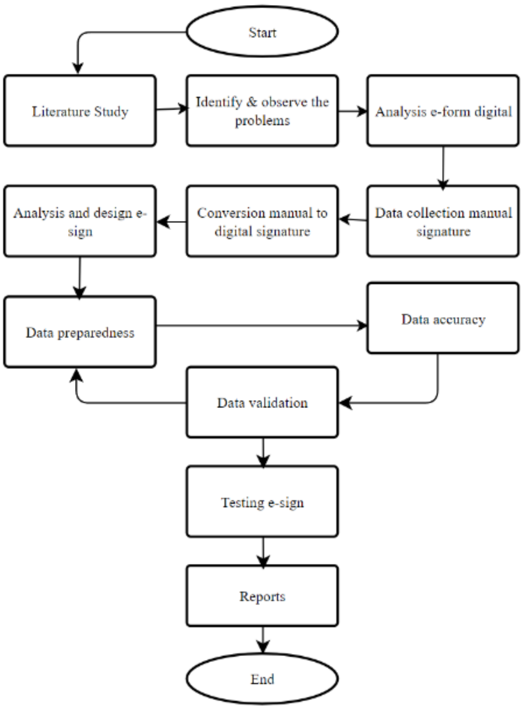

Start
Literature Study
Identify & observe the problems
Analysis e-form digital
Data collection manual signature
Conversion manual to digital signature
Analysis and design e-sign
Data preparedness
Data accuracy
Data validation
Testing e-sign
Reports
End

Figure 2. The research methods phase

3.3. Analysis of e-form Application

The e-form application is available, but the digital signature function has not been implemented. Signature characteristics are unique to each individual and impossible to duplicate. Signature verification systems are available on various platforms and technologies. The type of digital signature is divided into two methods, namely online and offline [25]. The online method utilizes electronic and computer techniques to extract information about the signature and retrieve dynamic information such as pressure, velocity, writing speed, and so on. On the other hand, offline methods involve less control and more use of images of signatures obtained by scanners or cameras. In signature verification with this offline method, the system uses features that have been extracted from scanned signature images. The features used with the offline method are also simpler because they only use pixels from the signature being evaluated.

System analysis of the e-form application to study the process of how digital signature will be done with the right system flow and algorithm on the Android application and produce a digital image on the mobile device screen The analysis involved examining the characteristics of signatures on various devices, including the type, brand, and detailed specifications of mobile devices used in the e-form application, such as the operating system, screen size, and storage capacity. Key aspects such as the canvas size for signatures, the extension of the digital images produced, and their aspect ratios were also assessed.

3.4. Design and Development of digital signature system

The DS process (digital signature) is carried out on the e-form application with the appropriate configuration. The owner and customer previously used offline methods, and it is possible to capture and record signatures on the Android screen (scanner) [26]. The signature process and each signature shape or stroke consisting of several pixels in the bitmap will be converted into an image in PNG format. Application development is carried out using the Mobile Application Development Life Cycle (MADLC) methodology stages: identification phase, design phase, development phase, prototyping phase, and testing phase. The application is also used to compare the digital image produced with the results of the manual signature process to see the level of similarity, quality, and size produced between the two [27]. The data collection process with the Advan iTab 7 Plus Tablet as the device requirement has a screen size of 7 inches with a screen pixel aspect ratio of 1280 x 720 (1280 pixels long, 720 pixels wide) with a diagonal of 7 inches (Table 1). Diagonal in pixels is calculated based on equation (3.1, 3.2., 3.3, 3.4):

Table 1. Formula image conversion

Equation	Noted
(3.1) $1\ \text{cm} = \frac{\text{DPI}}{1\ \text{inci}}$	where the inch in equation (3.1) can be converted into a centimetre unit, with the value: 1 inch = 2.54 cm.
(3.2) $\text{PPI} = \frac{\text{diagonal piksel}}{\text{diagonal inci}}$	To find the pixel size on a 1 cm device, the value of DPI/PPI value of the mobile device is calculated as (3.2); where the diagonal in pixels and the diagonal in inches in the equation are found using the Pythagoras Theorem.
(3.3) $\text{diagonal piksel} = \sqrt{x^2 + y^2}$	where x is the width of the device screen aspect ratio in pixels and y is the length of the device screen aspect ratio in equation (3.3).
(3.4) $\text{diagonal inci} = \sqrt{a^2 + b^2}$	where a is the width of the physical size of the device screen and b is the length of the physical size of the device screen in equation (3.4).
$\text{diagonal piksel} = \sqrt{x^2 + y^2}$ $\text{diagonal piksel} = \sqrt{720^2 + 1280^2}$ $\text{diagonal piksel} = \sqrt{518{,}400 + 1{,}638{,}400^2}$ $\text{diagonal piksel} = \sqrt{2{,}156{,}800}$ $\text{diagonal piksel} = 1{,}468.60$	With the known pixel diagonal = 1,468.60 and the diagonal inches = 7, find the DPI/PPI value based on equation (3.2):
$\text{DPI/PPI} = \frac{\text{diagonal piksel}}{\text{diagonal inci}}$ $\text{DPI/PPI} = \frac{1{,}468.60}{7}$ $\text{DPI/PPI} = 209.8$ $\text{DPI/PPI} \approx 210$	The DPI/PPI value of the Advan iTab 7 Plus is 210, and can be categorized into the HDPI model.
$1\ \text{cm} = \frac{\text{DPI}}{\text{inci}}$ $1\ \text{cm} = \frac{210}{1\ \text{inci}}$ $1\ \text{cm} = \frac{210}{2.54}$ $1\ \text{cm} = 82.67 \approx 83$	Each 1 cm of the screen consists of ± 83 pixels and has a DPI/PPI value of 210 then the DS model (digital signature), can be known.
$3\ \text{cm} \cong \frac{250\ \text{px}}{83\ \text{px}}$ $4\ \text{cm} \cong \frac{333\ \text{px}}{83\ \text{px}}$	Model 1, measuring 250 (length) x 333 (width) px, will be equivalent to a manual signature of size 3 (length) x 4 (width) cm if the calculation is based on the equation (3.1): 3 cm ≅ 250 px 83 px and 4 cm ≅ 333 px 83 px
$3\ \text{cm} \cong \frac{250\ \text{px}}{83\ \text{px}}$ $4.5\ \text{cm} \cong \frac{375\ \text{px}}{83\ \text{px}}$	Model 2, measuring 250 (length) x 375 (width) px will be equivalent to a manual signature with a size of 3 (length) x 4.5 (width) cm when calculations are made based on equation (3.1): 3 cm ≅ 250 px 83 px and 4.5 cm ≅ 375 px 83 px
$3\ \text{cm} \cong \frac{250\ \text{px}}{83\ \text{px}}$ $5\ \text{cm} \cong \frac{417\text{px}}{83\ \text{px}}$	Model 3, measuring 250 (length) x 417 (width) px, will be equivalent to a manual signature of size 3 (length) x 5 (width) cm if the calculation is done based on equation (3.1):3 cm ≅ 250 px 83 px, and 5 cm ≅ 417 px 83 px.

After successful retrieval data, the signature image is converted and resized into ½ the size of the signature model in PDF form. Comparative analysis of the model determines whether the digital signature and manual meet the similarity or suitability according to predetermined parameters.

Respondents will also fill out a questionnaire containing questions between signatures performed digitally and manually.

3.5. Data Collection and Conversion

Digital signature data collection was conducted through the application and manually using paper. A questionnaire was filled out by 20 respondents. Digital and manual signature samples were collected three times with different sizes of container models (canvas and field). Manual signature data was divided into three models with different sizes: 3x4 cm, 3x4.5 cm, and 3x5 cm. Similarly, the DS data was collected with three different pixel sizes: 250x333 px, 250x375 px, and 250x417 px.

3.6. Data Analysis

Each piece of data collected was carefully checked to ensure there were no defective parts or errors. The data were then recorded and separated or classified based on the signature model and aspect ratio, with particular attention to the metadata generated. The data categorization was done according to model, aspect ratio, and image storage size.

The analysis process involved calculating the frequency of the data size interval resulting from the generated system for each class model and aspect ratio of the image. Statistical methods used included:

- Descriptive Statistics: Basic statistical measures were used to summarize the data, such as mean, median, mode, and standard deviation.
- Comparative Analysis: Data sets were compared to identify patterns and trends, particularly between digital and manual signatures.

Questionnaire data was processed using a Likert scale of 1-5 to compare user satisfaction and perceptions of digital versus manual signatures. Responses were analyzed to identify trends and insights into user preferences and digital signatures' perceived reliability and usability.

3.7. Digital signature System Testing

Testing is carried out to determine whether there are still problems (errors or bugs) that need to be repaired thoroughly so it can be used for data collection. The Black-Box Testing method is used for all cases on the system. System testing was conducted to evaluate the performance and reliability of the digital signature application:

- Functional Testing: Ensured that all features of the application worked as intended.
- Performance Testing: Assessed the speed and efficiency of the application under different conditions.
- Usability Testing: Gathered feedback from users to improve the overall user experience.

3.8. Data Accuracy and Validation

The appropriate signature model or configuration implemented in the e-form application. Testing and validation were conducted to ensure that the quality level and storage size were optimal. The current signature model was compared to the manual process to check for improvements.

Validation processes were implemented to ensure the reliability and validity of the results:

- Internal Validation: Cross-checked data within the system to ensure consistency.
- External Validation: Compared the system’s output with manual signatures to ensure accuracy.
- Peer Review: Data and findings were reviewed by independent experts to validate the methodology and results. The appropriate signature model or configuration was implemented in the e-form application. Testing and validation were conducted to ensure that the quality level and storage size were optimal. The current signature model was compared to the manual process to check for improvements.

3.9. Report Preparation

A detailed report was prepared documenting the research methodology, data collection procedures, data analysis methods, system testing results, and validation processes. The report also includes a comprehensive discussion of the findings and their implications for the implementation of the digital signature system in the e-form application.

3.*10. Research Testing Device Specifications*

The software and hardware used are as follows: a. Microsoft Windows 8.1 Pro 64-Bit Operating System; b. Android Studio v.3.3; c. CorelDRAW X7; d. Notepad++, and e. Android OS 7.0 Nougat. Furthermore, the hardware specifications used to build is ASUS X450JB with following: Processor Intel® Core™ i7-4270HQ CPU @ 2.60GHz; Memory 12288MB RAM; 1 TB HDD Storage; NVIDIA GeForce 940M, and 14 inch monitor.

3.11. Testing Fumida digital signature System Application

Devices used for testing Fumida digital signature application: Tablet of Advan iTab 7 Plus type; including: Android OS 7.0 Nougat; 1.25GHz Quad-Core Processor; Memory 2GB RAM; 16GB storage, and Display 7 inch HD Screen (1280 x 720) IPS.

4. Result and Discussion

The digital signature application operates in accordance with the procedure, which requires the user to check in before the survey form menu appears. When touched, the screen will turn black, forming a line similar to a pen ready to scribble on paper, from white as a column or container (canvas). If something goes wrong, the process can be redone, erased, and saved as a PNG picture. An image of the signature on a form page will be displayed on the screen. The digital signature process flows from the e-form in this way: the size of the container/column (canvas/field), the image's extension and aspect ratio, the storage capacity, and the quality of the final signature image are all examined in the e-form system digital signature process flow. Using the stock Android operating system model, a screenshot and the canvas screen size are cropped with the signature image. Using the Microsoft Paint program, cut (crop) photos (Fig. 3). Through data information (metadata), the aspect ratio and image. size are visible.

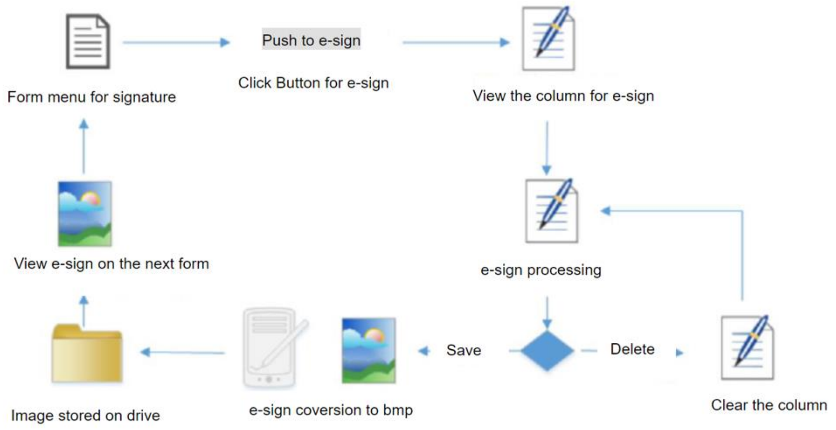
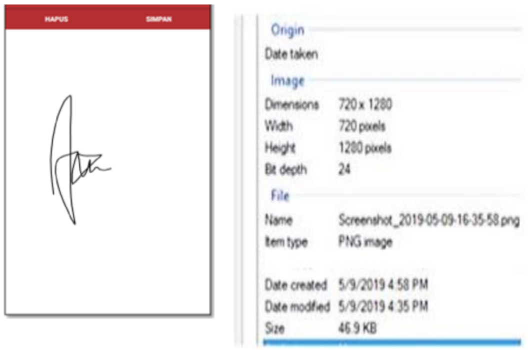


Figure 3. Fumida digital signature systems process flow

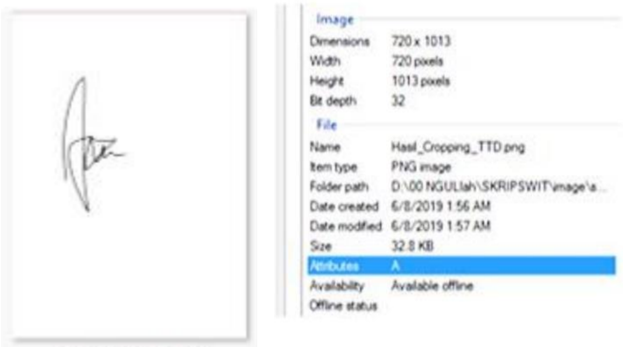
According to the screen of the Advan iTab 7 Plus mobile tablet, Figure 4 displays the data information (metadata) of the screenshot image with dimensions of 1280 x 720 (720 pixels image width, 1280 pixels image length). This metadata provides crucial details about the captured screenshot. Figure 5 shows the cropped image metadata from a screenshot of 1013 x 720 (1013 pixels wide, 1013 pixels long). It also illustrates the system's signature, indicating that the picture was changed into a Portable Network Graphics (PNG) bitmap form. Figure 5 shows the cropped image metadata from a screenshot of 1013 x 720 (1013 px wide, 1013 px long). Figure 5 shows the signature that the system generated as well as data information (metadata) indicating that the picture was changed into a PNG bitmap form. The final image has a storage capacity of 18.8 KB and an aspect ratio of 1013 x 720 (720 pixels wide, 1013 pixels long).



```
Origin
Date taken
Image
Dimensions     720 x 1280
Width          720 pixels
Height         1280 pixels
Bit depth      24
File
Name           Screenshot_2019-05-09-16-35-58.png
Item type      PNG image

Date created   5/9/2019 4:58 PM
Date modified  5/9/2019 4:35 PM
Size           46.9 KB
```

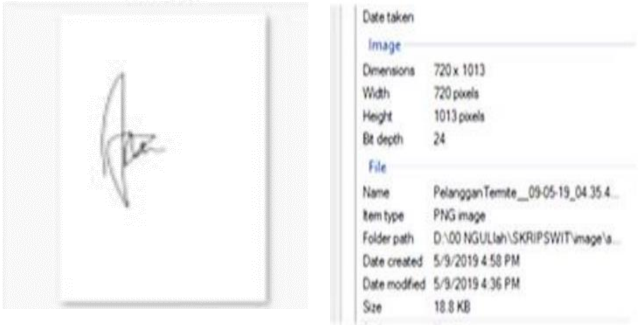
Figure 4. Data information from the screenshot



```
Image
Dimensions     720 x 1013
Width          720 pixels
Height         1013 pixels
Bit depth      32
File
Name           Hasil_Cropping_TTD.png
Item type      PNG image
Folder path    D:\00 NGULIah\SKRIPSWIT\image\a...
Date created   6/8/2019 1:56 AM
Date modified  6/8/2019 1:57 AM
Size           32.8 KB
Attributes     A
Availability   Available offline
Offline status
```

Figure 5. Information on data from cropping screen/canvas

Figure 6 depicts the image of the signature resulting from the conversion. If a bitmap type image with a large aspect ratio is reduced (resized) to a specified size, the image will be compressed into several pixels with a smaller size. The resolution becomes smaller and has the effect of reducing quality, as shown in Figure 6 and 7, which depicts the image of the digital signature when reduced to a certain size.



```
Date taken
Image
Dimensions     720 x 1013
Width          720 pixels
Height         1013 pixels
Bit depth      24
File
Name           PelangganTernite__09-05-19_04.35.4...
Item type      PNG image
Folder path    D:\00 NGULIah\SKRIPSWIT\image\a...
Date created   5/9/2019 4:58 PM
Date modified  5/9/2019 4:36 PM
Size           18.8 KB
```

Figure 6. Image of the signature resulting the conversion

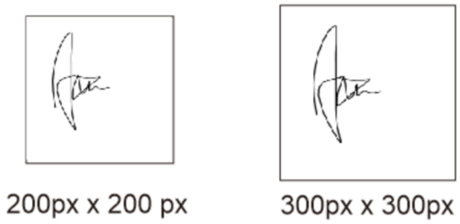


Figure 7. Image of the digital signature when reduced to a certain size

According to [28] prototype of the screen/canvas menu for entering signature data is shown in Figures 8 and 9. It serves the same purpose but differs in length and breadth. The signature can be reprocessed using the "Clear digital signature" tool, or it can be saved and converted to a PNG image using the "Save digital signature" tool. A prototype with a 250 x 333 pixel signature data filling screen/canvas is shown in Figure 9. A 250 x 375 pixel canvas is used in Figure 8's screen display/canvas to fill in the signature data for Model 2. Figure 9 displays the screen prototype/signature canvas size of 250px x 417px for Model 3 and the image conversion results (digital signature). The outcome of transforming the digital signature image into PNG format is displayed in Figure 9. To prevent misuse, the folder containing signature data is closed (hidden) for security reasons [29], though it can be changed using file manager settings. A prototype menu with comprehensive personal data and signature information is displayed in Figure 10. The relevant column will be filled up with the database's stored data. When users click the "Save to PDF" button, the data that is displayed will be converted into PDF format and stored in the device's memory by the system. The application system will restrict users from taking screen grabs in order to maintain security [30] [31]. The result of the conversion to PDF after clicking the "Save to PDF" option is shown in Figure 11.

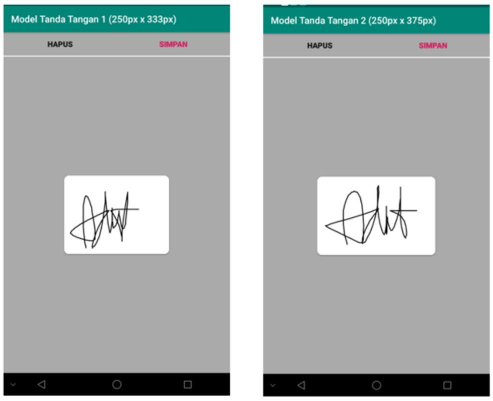
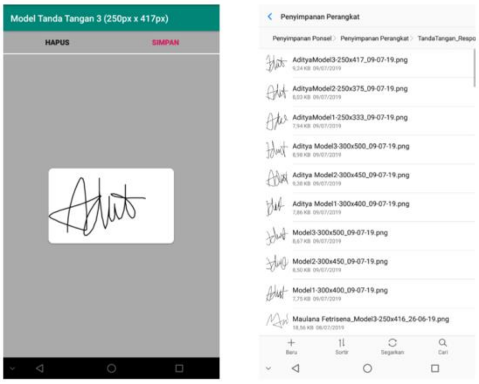

Model Tanda Tangan 1 (250px x 333px)
HAPUS
SIMPAN
Model Tanda Tangan 2 (250px x 375px)
HAPUS
SIMPAN

Figure 8. Prototype Screen/Signature Canvas size 250px x 333px and 250px x 375px



Penyimpanan Ponsel > Penyimpanan Perangkat > TandaTangan_Respo

AdityaModel3-250x417_09-07-19.png
9,24 KB 09/07/2019

AdityaModel2-250x375_09-07-19.png
8,03 KB 09/07/2019

AdityaModel1-250x333_09-07-19.png
7,94 KB 09/07/2019

Aditya Model3-300x500_09-07-19.png
6,98 KB 09/07/2019

Aditya Model2-300x450_09-07-19.png
9,38 KB 09/07/2019

Aditya Model1-300x400_09-07-19.png
7,86 KB 09/07/2019

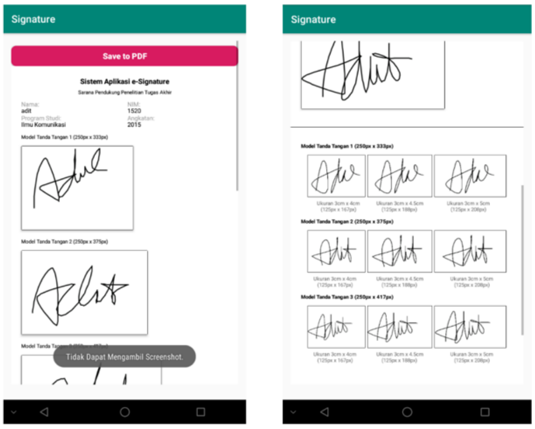
Model3-300x500_09-07-19.png
8,67 KB 09/07/2019

Model2-300x450_09-07-19.png
8,50 KB 09/07/2019

Model1-300x400_09-07-19.png
7,75 KB 09/07/2019

Maulana Fetrisena_Model3-250x416_26-06-19.png
18,56 KB 08/07/2019

Figure 9. Screen Prototype/Signature Canvas size 250px x 417px and Image Conversion Results (digital signature)



Sistem Aplikasi e-Signature
Sarana Pendukung Penelitian Tugas Akhir

Nama: adit
NIM: 1520
Program Studi: Ilmu Komunikasi
Angkatan: 2015

Model Tanda Tangan 1 (250px x 333px)

Model Tanda Tangan 2 (250px x 375px)

Model Tanda Tangan 1 (250px x 333px)

Ukuran 3cm x 4cm (125px x 167px) | Ukuran 3cm x 4.5cm (125px x 188px) | Ukuran 3cm x 5cm (125px x 208px)

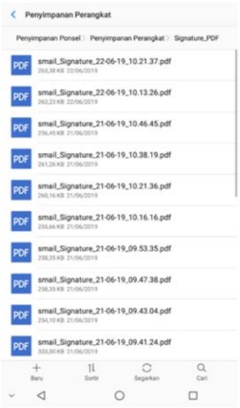
Model Tanda Tangan 2 (250px x 375px)

Ukuran 3cm x 4cm (125px x 167px) | Ukuran 3cm x 4.5cm (125px x 188px) | Ukuran 3cm x 5cm (125px x 208px)

Model Tanda Tangan 3 (250px x 417px)

Ukuran 3cm x 4cm (125px x 167px) | Ukuran 3cm x 4.5cm (125px x 188px) | Ukuran 3cm x 5cm (125px x 208px)

Figure 10. Detailed Prototype of Personal Data Information and digital signature



Penyimpanan Ponsel > Penyimpanan Perangkat > Signature_PDF

smail_Signature_22-06-19_10.21.37.pdf
263,38 KB 22/06/2019

smail_Signature_22-06-19_10.13.26.pdf
263,23 KB 22/06/2019

smail_Signature_21-06-19_10.46.45.pdf
256,45 KB 21/06/2019

smail_Signature_21-06-19_10.38.19.pdf
261,26 KB 21/06/2019

smail_Signature_21-06-19_10.21.36.pdf
260,16 KB 21/06/2019

smail_Signature_21-06-19_10.16.16.pdf
255,66 KB 21/06/2019

smail_Signature_21-06-19_09.53.35.pdf
258,35 KB 21/06/2019

smail_Signature_21-06-19_09.47.38.pdf
258,35 KB 21/06/2019

smail_Signature_21-06-19_09.43.04.pdf
254,10 KB 21/06/2019

smail_Signature_21-06-19_09.41.24.pdf
333,00 KB 21/06/2019

Figure 11. Results of Conversion of Personal Data and digital signature

Eleven test cases comprise the black-box testing approach used to test the digital signature. With the "TRUE" indicator, every test case yields the actual result as expected. Therefore, it can be said that the digital signature's system and functional code has been operating as intended. On a sample of twenty-two responders, digital signature and manual data collection were performed three times for each model using varying container sizes (canvas/field). During the data retrieval procedure, no flaws or problems were discovered in the data, particularly in the digital signature results that were converted into PNG format. With various outputs, the data yielded 66 signatures. The data can be divided or categorized based on the model/image aspect ratio size of each signature to determine the data size. model.

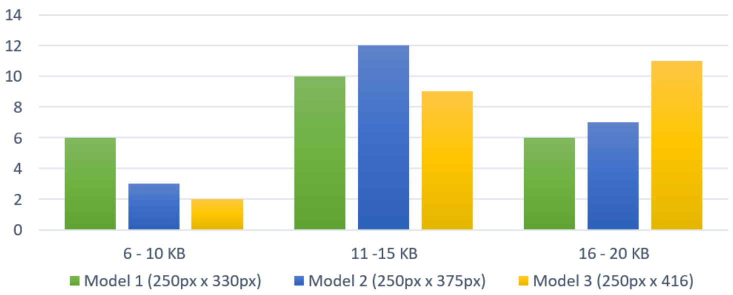


Figure 12. Comparison of Data Size Results for Signature Model 1, 2 and 3

The cross-tabulation results between the signature model and data size (in KB) are shown in Figure 12. 11 data are in the range, with 6 data model 1 (250 px x 330 px), 3 data model 2 (250 px x 375 px), and 2 data model 3 (250 px x 416 px), according to the data size attribute/data size interval 6-10 KB. With 10 data model 1 (250 px x 330 px), 12 data model 2 (250 px x 375 px), and 9 data model 3 (250 px x 416 px), there are 31 data in the range. There are 24 data with 6 data model 1 (250 px x 330 px), 7 data model 2 (250 px x 375 px), and 11 data model 3 (250 px x 416 px) inside the 16–20 KB interval.

The minimum values chosen for the results in this study are based on the requirements and constraints identified during the literature study and observational analysis at PT Fumida Pestindo Jaya. These values were determined by considering the following factors:

1. User Acceptance and Usability: The minimum values were chosen to ensure user acceptance and usability of the digital signature application. The usability testing methodology described by Rubin & Chisnell (2008) in “Handbook of Usability Testing” was followed, which helped in identifying the acceptable range of values for various parameters. This approach ensures that the chosen minimum values are user-friendly and meet the practical needs of the end-users.
2. Technical Specifications and Device Constraints: The technical specifications of the devices used, such as the Advan iTab 7 Plus Tablet, were considered to determine the minimum values. The device’s screen size, resolution, and DPI/PPI values played a crucial role in setting the minimum values for signature capture and processing. These values were calculated based on the equations provided in the “Design and Development of digital signature System” section.
3. Comparative Analysis: A comparative analysis was conducted between the manual and digital signatures. The minimum values were set to ensure that the digital signatures closely match the manual signatures in terms of quality and size. This comparison ensures that the digital signatures are reliable and acceptable as per the predefined parameters.
4. Empirical Data and Observations: The empirical data collected from user feedback and system logs during the observational study were analysed to determine the minimum values. This data provided insights into the practical limitations and requirements of the users, helping in setting realistic and appropriate minimum values.

By considering these factors, the minimum values chosen for the results were justified and deemed appropriate for ensuring the effectiveness and usability of the digital signature application. According to survey respondents, 76.81% of them agreed that digital signature technology can mimic, match, or reflect manual (paper) signatures. With a proportion of 72.72% (16 respondents), the majority of respondents believed that digital signatures can be used in place of manual (paper) signatures. Just 13.64% (3 respondents) strongly agreed, compared to 9.09% (2 respondents) and 4.55% (1 respondent) who disagreed with the remaining responses. With a proportion of 79.09% (scoring 87), it is evident from the sample that most respondents felt that digital signatures can resemble manual (paper) signatures. Aside from that, 72.72% (16 respondents) and 4.45% (1 respondent) strongly agreed that the digital signature was comparable to and/or compatible with manual (paper) signatures. Subsequently, 13.64% (3 respondents) gave neutral responses, while 9.09% of respondents disagreed. The second questionnaire item yielded a total score of 74.55%, or 82%.

Results of data collection on respondents' perceptions of the digital signature's accuracy showed that, of the three questionnaire items that were already in place, 73.33% of respondents agreed that the three signature models in the digital signature had a degree of accuracy and/or conformity with manual (paper) signatures, though some respondents disagreed. 9 respondents, or 40.91% of the total, agreed that the signature model 1 digital signature is accurate and/or conforms to some extent to manual (paper) signatures. Subsequently, there was minimal variation in the responses indicating neutrality (31.82%; 7 respondents) and disagreement (27.27%; 6 respondents).

The final score, which fell into the agree category, had a percentage of 62.73% (score 69). Additionally, with reference to signature model 2, a total of 13 respondents, or 59.09%, expressed agreement that the model's accuracy and/or conformance to manual (paper) signatures was satisfactory, and three respondents, or 13.64%, strongly agreed. the. Nonetheless, 18.18% (4 respondents) of the respondents gave a neutral response, while 2.9% of the respondents disagreed. With a percentage of 75.46% (score 83), the final score was attained and it fell into the agree category. Subsequently, regarding signature model 3, up to 50% (11 respondents) expressed agreement with the model's correctness and/or suitability for manual (paper) signatures, with 31.82% (7 respondents) strongly agreeing. Nonetheless, a number of respondents indicated they had no opinion, with 13.64 (3 respondents) and 4.55% (1 respondent) indicating they disagreed. With a final percentage of 81.82% (score 90), the score fell into the agree category. Compared to the other two signature models, namely signature model 1 (62.73%) and signature model 2 (75.46%), it is evident from the explanation above that signature model 3 has the highest proportion, at 81.82%. Thus, compared to other signature models, it is evident that signature model 3 in the digital signature has a higher degree of accuracy and/or conformance with manual (paper) signatures. The outcomes of this score serve as proof that the DS can accurately replicate the original signature (manually) by identifying the model or configuration of the DS (digital signature) that is appropriate for use or integration into the e-form application.

Regarding the digital signature quality level indicators, 68.79% of respondents agreed—though some respondents disagreed—that the signature results from the three signature models in the digital signature were not broken, ghosted, and/or dotted when reduced (resized) to the size model that has been determined. This was based on responses to the three existing questionnaire items. When reduced (resized) to the designated model size, the signature picture generated from signature model 1 is neither damaged, ghosted, or dotted, according to the answer score of 59.09% (13 respondents). Subsequently, 9.09% (2 respondents) expressed strong agreement with this, which is not significantly different from the responses that claimed they were indifferent (18.18% (4 respondents), disagreed (9.09% (2 respondents), and strongly disagreed (4.55% (1 respondent)).

The final score, which fell into the agree category, had a percentage of 71.82% (score 79). Additionally, when reduced (resized) to the necessary model size, 59.09% of respondents (13 respondents) agreed that the signature picture generated from this signature model was not broken, ghosted, or dotted. On the other hand, 18.18% of respondents disagreed, 4.55% of respondents strongly disagreed, and 18.18% of respondents answered in a neutral manner. With a percentage of 66.36% (score 73), the final score was attained and it was classified as agree. Subsequently, for signature model 3, a total of 10 respondents, or 45.45%, concurred that the resulting signature image exhibited a degree of precision and/or adherence to manual (paper) signatures. The percentage of 9.09% (2 respondents) who indicated they strongly agreed came next. A number of respondents, however, also expressed that they had no opinion; 22.73% (5 respondents) agreed, while 22.73% (5 respondents) disagreed. The final score, which fell into the agree category, had a percentage of 68.18% (score 75). Compared to the other two signature models, namely signature model 2 (66.36%) and signature model 3 (68.18%), the signature model 1 has the highest proportion, at 71.82%. In comparison to other signature models, it is evident that signature model 1 in the Fumida digital signature generates correctly when shrunk (resized) to the designated model size, ghosted and/or dotted. The score's findings provide proof for the research's main issue, which is making sure the DS can accurately represent the original signature (manually) by making sure the digital signature's output doesn't later change in form or content when it's integrated into an e-form application.

According to data collected from respondents on e-comparison indicators, 8 respondents, or 36.36% of the total, agreed that the signature image generated by signature model 1 is of higher quality and similarity than images produced by other signature models. 9.09% of the respondents (2 people) then said that they strongly agreed with this. Additionally, a proportion of 31.82 (7 respondents) indicated disagreement, while a percentage of 22.73% (5 respondents) gave neutral responses. The final score, which fell into the agree category, had a percentage of 64.54% (score 71). Additionally, of the respondents to signature model 2, 36.36% (8 respondents) felt that the final signature image was of higher quality and resemblance than the signatures from the previous signature models. A highly agree response, with a proportion of 13.64% (3 respondents), came next. On the other hand, 2 respondents (9 respondents) disagreed and 40.91% of respondents reacted neutrally. The final score, which fell into the agree category, had a percentage of 70.91% (score 78). Subsequently, regarding signature model 3, 8 respondents (36.36%) concurred that, in comparison to previous signature models, the signature image generated by this model was of higher quality and likeness.

A further percentage of 31.82% (7 respondents) said that they strongly agreed with this. Nonetheless, a number of respondents had a neutral stance on the matter, with 13.64% (3 respondents) and 18.18% (4 respondents) expressing disagreement. The final score, which fell into the agree group, had a percentage of 76.36% (score 84). According to the explanation given above, of the two signature models—Signature Model 1 (64.54%) and Signature Model 2 (70.91%)—Signature Model 3 has the highest proportion, at 76.36%. As a result, it is evident that digital signature model 3 generates images that are more similar and of higher quality than those generated by previous signature models. The score's outcomes provide proof for the research's main issue, which is proving that DS can accurately reflect the original signature (manually) by making sure the model and configuration of DS (digital signature) are suitable for use in e-applications. Based on the separation/categorization of three indicators—the degree of digital signature accuracy, the quality level of digital signature, and comparison based on respective signature models—the four questionnaire indicators indicate that the digital signature model is similar to or conforms to a manually signed paper document.

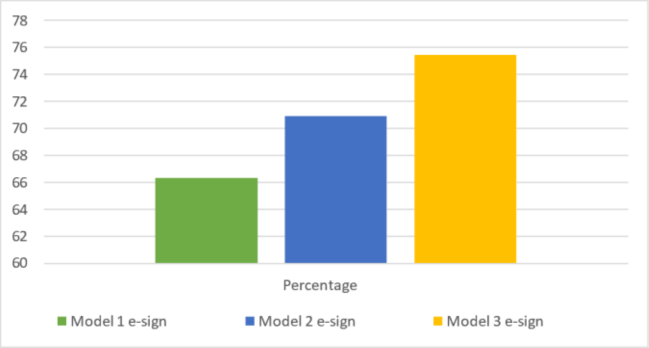


Figure 13. Bar Chart of Percentage Values for 1, 2 and 3 digital signature Models

Models 1 and 2 receive total scores of 66.36% (score 219), 70.91% (score 234), and 75.45% (score 249), respectively, based on the percentage findings. In terms of percentage level and score, the model 3 is superior. This is further supported by the fact that model 3's accuracy percentage is 81.82% (score 90), while digital signature 1's percentage is 76.36% (score 84). While signature model 1 has a higher percentage of digital signature quality (71.82%; score 79) than signature model 3 (68.18%; score 75), signature model 3 has a higher percentage overall. In comparison to the other models, Model 3, which measures 250 pixels in length and 417 pixels in width, is the most comparable to and conforms to a manual (paper) model. The fact that the average data size is 15 KB further supports this. The three models' average data sizes are 13 and 14 KB.

Refer to [32] data validation was accomplished by inserting the 250 (length) x 417 (width) px signature model 3 into the digital signature feature of the e-form application. The selection of the model is based on the outcomes of earlier data analysis. The screen/canvas size of the digital signature procedure for the e-form system has been changed to model 3, which has dimensions of 250 px for length and 417 px for width. The system-generated signature, which includes metadata, has a data size of 8.06 KB with an aspect ratio of 250 x 417 (250 pixels wide, 417 pixels wide). The image does not significantly lose quality despite the aspect ratio being scaled; it is free of shadows and unfinished (dotted) areas, and its quality is maintained in PDF format.

5. Conclusions

Our research has successfully improved the quality of the digital signature (digital signature) image by developing an Android application using the Mobile Application Development Life Cycle (MADLC) method for PT Fumida Pestindo Jaya (Fumida). This application functions as a replacement for paper media in the recording process for surveys, pest control, termite control, and/or fumigation.

Based on the analysis conducted, we found that the inaccuracy or decrease in the quality of the signature image produced by the previous application (e-form Fumida) when converted into Portable Network Graphics (PNG) format can be improved. Data collection was carried out for testing to determine the signature model that is in accordance with the parameters/indicators that have been determined. Calculation of questionnaire data was conducted to find the right configuration model to be implemented into e-form Fumida.

Our digital signature model performs best in terms of accuracy and data size. Specifically, Signature Model 3 demonstrated the highest degree of accuracy and conformance with manual (paper) signatures, achieving an accuracy rate of 81.82%. Additionally, this model maintained a manageable data size with an average of 15 KB.

To identify the optimal parameters for the digital signature model in future research, we suggest using systematic approaches such as:

1. Grid Search: Evaluates a range of parameter combinations systematically.
2. Bayesian Optimization: A probabilistic model-based optimization technique to efficiently search the parameter space.

The results show that the new digital signature system improves the accuracy and quality of digital signatures. Further optimization of the model's parameters can enhance its performance, providing a more reliable solution for digital signatures in various applications.

6. Limitations

This study has several limitations. Firstly, the sample size of respondents is relatively small, which may affect the generalizability of the findings. Additionally, the study is limited to the use of the Advan iTab 7 Plus Tablet, and the results may vary with different devices. The study also focuses on a specific application in a specific industry, which may not be representative of all potential use cases of digital signatures.

7. Future Work

Future research could explore the application of more advanced algorithms for signature capture and verification, as well as the integration of biometric features for enhanced security. Further studies could also investigate the user experience and adoption of digital signature in other industries. Future research should consider expanding the sample size and including a more diverse range of devices to validate the findings. Additionally, exploring the application of digital signatures in different industries and contexts could provide a broader understanding of their effectiveness and limitations. Further studies could also investigate the long-term usability and security aspects of digital signatures in various settings.

8. Acknowledgement

The author would like to thank Universitas Bakrie for the support during the research reported in this paper.

References

[1] A. A. Santosa *et al.*, ‘How the COVID-19 Pandemic Affected the Sustainable Adoption of Digital Signature: An Integrated Factors Analysis Model’, *Sustainability (Switzerland),* vol. 14, no. 7, 2022, doi: 10.3390/su14074281.

[2] T. Bálint and J. Bucko, ‘Comparative Analysis of Handwritten, Biometric and Digital Signature’, *International Review of Social Sciences and Humanities*, vol. 4, no. 2, 2013.

[3] M. Levi-Bliech, P. Kurtser, N. Pliskin, and L. Fink, ‘Mobile apps and employee behavior: An empirical investigation of the implementation of a fleet-management app’, *Int J Inf Manage,* vol. 49, 2019, doi: 10.1016/j.ijinfomgt.2019.07.006.

[4] M. Cristofaro, ‘E-business evolution: an analysis of mobile applications’ business models’, *Technol Anal Strateg Manag,* vol. 32, no. 1, 2020, doi: 10.1080/09537325.2019.1634804.

[5] P. Weichbroth and Ł. Łysik, ‘Mobile Security: Threats and Best Practices’, *Mobile Information Systems,* vol. 2020. 2020. doi: 10.1155/2020/8828078.

[6] C. Sybi, G. Mary, and P. M. D. Julia, ‘A survey on android mobile based application and its security’, *i-manager’s Journal on Mobile Applications and Technologies*, vol. 9, no. 1, 2022, doi: 10.26634/jmt.9.1.18910.

[7] K. L. Kettle and A. Mantonakis, ‘Look for the signature: Using personal signatures as extrinsic cues promotes identity-congruent behavior’, *J Bus Res,* vol. 170, 2024, doi: 10.1016/j.jbusres.2023.114353.

[8] M. A. K. Et. al., ‘Analysis and Design of Mobile-Based Waste Management Applications Prototype Methods’, *Turkish Journal of Computer and Mathematics Education (TURCOMAT),* vol. 12, no. 4, 2021, doi: 10.17762/turcomat.v12i4.556.

[9] P. Deepa, ‘Design and Development of Mobile Application for Waste Management’, *Int J Res Appl Sci Eng Technol*, vol. 8, no. 8, 2020, doi: 10.22214/ijraset.2020.30930.

[10] K. Henrys, ‘Mobile application model for solid waste collection management’, *SSRN Electronic Journal*, 2021, doi: 10.2139/ssrn.3808542.

[11] T. Bálint and J. Bucko, ‘Comparative Analysis of Handwritten, Biometric and Digital Signature’, *International Review of Social Sciences and Humanities*, vol. 4, no. 2, 2013.

[12] A. A. Santosa *et al.*, ‘How the COVID-19 Pandemic Affected the Sustainable Adoption of Digital Signature: An Integrated Factors Analysis Model’, *Sustainability (Switzerland)*, vol. 14, no. 7, 2022, doi: 10.3390/su14074281.

[13] M. Levi-Bliech, P. Kurtser, N. Pliskin, and L. Fink, ‘Mobile apps and employee behavior: An empirical investigation of the implementation of a fleet-management app’, *Int J Inf Manage*, vol. 49, 2019, doi: 10.1016/j.ijinfomgt.2019.07.006.

[14] U. Yu. Akhundjanov and V. V. Starovoitov, ‘On the invariance of the digital description of a handwritten signature’, *«System analysis and applied information science»*, no. 4, pp. 47–55, Feb. 2023, doi: 10.21122/2309-4923-2022-4-47-55.

[15] A. Mendaza-Ormaza, O. Miguel-Hurtado, R. Blanco-Gonzalo, and F. J. Diez-Jimeno, ‘Analysis of handwritten signature performances using mobile devices’, in *Proceedings - International Carnahan Conference on Security Technology*, 2011. doi: 10.1109/CCST.2011.6095930.

[16] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering*. Wiley, 2015. doi: 10.1002/9781118722367.

[17] M. Cristofaro, ‘E-business evolution: an analysis of mobile applications’ business models’, *Technol Anal Strateg Manag*, vol. 32, no. 1, 2020, doi: 10.1080/09537325.2019.1634804.

[18] D. P. Franco, F. D. Barboza, and N. M. Cardoso, ‘A secure method for authenticity verification of handwritten signatures through digital image processing and artificial neural networks’, *International Journal of Communication Networks and Information Security*, vol. 5, no. 2, 2013, doi: 10.17762/ijcnis.v5i2.382.

[19] F. E. Batool *et al.*, ‘Offline signature verification system: a novel technique of fusion of GLCM and geometric features using SVM’, *Multimed Tools Appl*, 2020, doi: 10.1007/s11042-020-08851-4.

[20] X. Huang, Y. Dong, G. Ye, W. S. Yap, and B. M. Goi, ‘Visually meaningful image encryption algorithm based on digital signature’, *Digital Communications and Networks*, vol. 9, no. 1. 2023. doi: 10.1016/j.dcan.2022.04.028.

[21] P. Weichbroth and Ł. Łysik, ‘Mobile Security: Threats and Best Practices’, *Mobile Information Systems*, vol. 2020. 2020. doi: 10.1155/2020/8828078.

[22] T. Vithani and A. Kumar, ‘Modeling the mobile application development lifecycle’, in *Lecture Notes in Engineering and Computer Science*, 2014.

[23] T. Vithani and A. Kumar, ‘Modeling the mobile application development lifecycle’, in *Lecture Notes in Engineering and Computer Science*, 2014.

[24] X. Huang, Y. Dong, G. Ye, W. S. Yap, and B. M. Goi, ‘Visually meaningful image encryption algorithm based on digital signature’, *Digital Communications and Networks*, vol. 9, no. 1. 2023. doi: 10.1016/j.dcan.2022.04.028.

[25] P. V Hatkar and Z. J. Tamboli, ‘Image Processing for Signature Verification’, *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)*, no. 3, pp. 2347–5552, 2015.

[26] L. Ma, L. Gu, and J. Wang, ‘Research and development of mobile application for android platform’, *International Journal of Multimedia and Ubiquitous Engineering*, vol. 9, no. 4, pp. 187–198, 2014, doi: 10.14257/ijmue.2014.9.4.20.

[27] J. Zimmer *et al.*, ‘The challenge of comparing digitally captured signatures registered with different software and hardware’, *Forensic Sci Int*, vol. 327, 2021, doi: 10.1016/j.forsciint.2021.110945.

[28] M. A. Kusmawardani, ‘Analysis and Design of Mobile-Based Waste Management Applications Prototype Methods’, *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, pp. 723–733, 2021, doi: 10.17762/turcomat.v12i4.556.

[29] E. Y. Chou, ‘What’s in a name? The toll digital signatures take on individual honesty’, *J Exp Soc Psychol*, vol. 61, pp. 84–95, 2015, doi: 10.1016/j.jesp.2015.07.010.

[30] P. Weichbroth and Ł. Łysik, ‘Mobile Security: Threats and Best Practices’, *Mobile Information Systems*, vol. 2020, 2020, doi: 10.1155/2020/8828078.

[31] F. Zou, S. Zhang, T. Wan, and L. Pan, ‘A survey of android mobile platform security’, in *10th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2014)*, 2014, pp. 520–527. doi: 10.1049/ic.2014.0155.

[32] K. A. Adeniji, N. T. Surajudeen-Bakinde, O. O. Omitola, and A. Ajibade, ‘Validation of android-based mobile application for retrieving network signal level’, *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, pp. 296–304, 2021, doi: 10.11591/ijeecs.v21.i1.pp296-304.