Development of a tool for determining the authenticity of signature using the raspberry pi board

D H Rohan, M Yusrö* and W Djatmiko
Faculty of Engineering, Universitas Negeri Jakarta, Jakarta, Indonesia

*myusro@unj.ac.id

Abstract. Determining the authenticity of signatures is an important task in office / company administration because there are many cases of counterfeiting. The purpose of this study is to develop a tool for determine the authenticity of signature based. The device consists of three main parts, namely a camera module for reading signature images, a raspberry pi board for processing signature images; and an LCD module for displaying the results of signature authenticity detection. This study proposes a simple algorithm using the binary image method and canny edge detection to change images and compare pixel values between reference signature images and doubtful signature images. This process is done by comparing pixels with the same position from different signature images. The comparison results will base for the tool to determine the authenticity of signatures. The result is displayed on the LCD screen with the name of the owner of the signature obtained from the tool database. This system can store five signatures that serve as reference signatures and has six possible final decisions in determining the authenticity of signatures. The results showed that the system can determine the authenticity of signatures with a success rate of 82% from testing of ten different signature images.

1. Introduction
In an organization or company, a signature is important and crucial in administration. A signature is a form of legalization of a letter or decision from an organization or company. Crimes that often arise related to signatures are falsification of signatures. For example, a case published in the media www.thedailybeast.com that published case of signature forgery in an arrest and deportation warrant in the Immigration and Customs Deportation section in Little Rock, Arkansas [1].

In Indonesia, falsification of signatures has been regulated in the Indonesian Criminal Code (KUHP), article 263 verse (1) which reads "Anyone who makes a fake letter or falsifies a letter, who can issue rights, agreements (obligations) or debt relief, or which can be used as an explanation for an action, intending to use or order someone else to use the document as if the document is genuine and not falsified, then using it may result in the loss of the penalty for forgery of the letter, with a sentence of up to six years in prison " [2].

Generally, there are two ways to prevent signature forgery [3]. The first method is by manually checking by the administrative officer by seeing and matching the doubtful signature with the original signature of the official of the organization or company. The second way is to ask the officials about the signature. However, along with the development of information technology, the forgery of signatures is increasingly sophisticated. Fake signatures often resemble even the same as the original signature. Often administrative staff finds it difficult to determine the authenticity of signatures. Determination of the
The authenticity of a signature is a visual work, in which the direction of the signature line must be certain to determine the authenticity of the signature.

The study of determining the authenticity of signatures has been done before by many people/institutions. Blankers et al held a competition about the authenticity of signatures aimed at combining realistic forensic casework with automated methods by testing a new system [4]. In 2011, Marcus Liwicki et al also made a competition with the title "Signature verification competition for online and offline skilled forgeries" which aimed to find a signature verification system that could be implemented in the forensic field [5]. Research on the authenticity of signatures was also carried out by Hayatunnufus et al to create a signature verification application program with a spatial domain image using the Summary Squared Error (SSE) method [6]. The results of the process will state the suitability of a signature. The test results show that the SSE can recognize signatures with a 96% accuracy in the sample data. Sandy et al have done research using the K-Nearest Neighbor classification method, because this method is more easily applied than other classification methods [7]. From the test results obtained by the quality level of the signature determination system using the SFET and MAP methods that are measured using an accuracy calculation that obtained an accuracy of 62 percent for 10 originals and non-authentic signatures of 5 people.

In general, from several studies that have been carried out, they have not used hardware or there are no tools made. This research aims to make a tool for determine the authenticity of signature based on image processing principles using raspberry pi [8]. This study proposes a simple algorithm using the binary image method and canny edge detection to change the image [9,10], and for comparison between reference signature images (original) with doubtful signature, images are done by comparing the pixel values with the same position of the reference signature images and doubtful signature image.

2. Methods
The research method chosen was research and development which included problem identification, product design to system testing and analysis. The device consists of three main parts, the camera module for capturing signature images; a raspberry pi module for processing signature images; and an LCD module to display the results of signature authenticity detection. All three are assembled into a system that can determine the authenticity of signatures using an algorithm to compare pixel values of signature images. The original signature image is converted to a binary image and canny image, the same is done with the doubtful signature image. The system will compare the two, the results of the comparison will determine the authenticity of the signature. The block diagram of the system can be seen in Figure 1.

![Figure 1. Block diagram of the system.](image)

In Figure 1, there are three sub-sections namely:

- The first is an input section consisting of a camera module, keyboard wireless, and receiver keyboard. The first sub-section functions as an input device for later processing by a raspberry pi. The camera module functions as a camera that is used to take pictures of signatures, be they reference signatures or doubtful signatures. The keyboard wireless functions as a device to enter a username after the reference signature image is taken.
The second section is raspberry pi as a processor system [11]. This section functions as an image input processor from the camera to save all signature images, saves the name of the signatory, and the last is processing the signature image until an authenticity decision is obtained from the doubtful signature.

The last is the output section which can be used also as an input namely an LCD touch screen. This sub-section functions as an interface device with the user and displays the results of comparing signatures.

3. Results and discussion

In general, the way to determine the authenticity of signatures is by taking two signature pictures and comparing them. The reference signature (original) will be captured with the first program and then the system will save the signature image after the image is saved, the system will ask for the name of the signature, and the last process is capturing the signature image that is doubtful with the second program.

The first image processing performed by the system is to change pictures taken from the reference signatures and images taken from the doubtful signature into a grayscale images (grayscale). The second image processing is to convert grayscale images into binary images. The third image processing is to convert grayscale images into Canny images. After doing three image processing, the system can run a comparison algorithm. This algorithm will compare pixel values with the same position in the two images (reference and image of the doubtful signature). The results of image processing by the tool can be seen in Table 1.

| Original | Grayscale | Binary | Canny Edge |
|----------|-----------|--------|------------|
| ![](image1.png) | ![](image2.png) | ![](image3.png) | ![](image4.png) |
| ![](image5.png) | ![](image6.png) | ![](image7.png) | ![](image8.png) |
| ![](image9.png) | ![](image10.png) | ![](image11.png) | ![](image12.png) |
| ![](image13.png) | ![](image14.png) | ![](image15.png) | ![](image16.png) |
| ![](image17.png) | ![](image18.png) | ![](image19.png) | ![](image20.png) |

In Table 1, there are 5 original images and 5 image processing results with 3 different methods, namely, grayscale images, binary images, and canny images. The system test will be used 10 times for each user, the image of the doubtful signature compared to the reference signature image (original) 5 times, and will be compared with the fake signature images 5 times as well, because the system capacity can only load as many as 5 users, then testing is done 50 times. The sample test results can be seen in Table 2.
Table 2. Sample test results of the system.

| No | Username | Compare With | System Decision |
|----|----------|--------------|-----------------|
| 1  | Denanda  | Real         | Match           |
| 2  | Denanda  | Fake         | Match           |
| 3  | Denyansyah | Real       | Match           |
| 4  | Denyansyah | Fake      | Match           |
| 5  | Andriany | Real         | Match           |
| 6  | Andriany | Fake         | Match           |
| 7  | Jawal    | Real         | Match           |
| 8  | Jawal    | Fake         | Match           |
| 9  | Darwin   | Real         | Not Match       |
| 10 | Darwin   | Fake         | Match           |

Table 2, there is a sample of data obtained by testing the signature authenticity tool. Reference signatures are compared with 10 signature samples, 5 original signature samples, and 5 fake signature samples; fake signatures obtained from signature forgers are done with the signature owner's approval. The results of testing the entire system determining the authenticity of signatures as much as 50 times showed an accuracy rate of 82% which means there is an 18% chance the system was wrong in determining the authenticity of signatures.

Signature authenticity tools have several needs in determining the authenticity of signatures, the requirements referred to include: the device must be able to hold the camera at the same distance from the signature when capturing images so that images will not be found with different sizes; the device must be able to support the camera in a still state while it is moving, and the lighting during capturing the signature process must be the same and stable, to prevent the lighting from changing, the surrounding camera will be closed and given two artificial light sources in the form of white LEDs.

Based on the need for a tool to determine the authenticity of a signature, a tool that can support all of these needs is made. The real tools that have been made in this study are shown in Figure 2.

Figure 2. A signature authenticity determination tool.

4. Conclusion
Based on testing that has been done 50 times and analysis of results of testing conducted overall tool then found the conclusion; there are two courses on the authenticity of the signature decisive tool based on processing the image using raspberry pi 3, a program to make a signature as a reference signature, and a program to determine the authenticity of a signature; signature authenticity can store 5 users; there
are 6 possible final decisions determined by the authenticity-based signature processing tool using raspberry pi 3, namely the original stated signature with reference signature 1, original declared signature with reference signature 2, original declared signature with reference signature 3, the signature is declared original with reference signature 4, the signature is declared original with reference signature 5, and the signature is declared false; and determination of signature authenticity tools based on image processing using raspberry pi can determine the authenticity of signatures with an accuracy of 82%, which means there is an 18% chance that these tools incorrectly determine signatures.

Acknowledgments
We would like to thank Universitas Negeri Jakarta, especially Department of Electrical Engineering, Faculty of Engineering, Universitas Negeri Jakarta for supporting this research.

References
[1] Barbie L N 2019 ICE Agents Forged Signatures, Skipped Review to Keep Migrants Detained: Report [Online] Retrieved from: https://www.thedailybeast.com/ice-agents-forged-signatures-skipped-review-to-keep-migrants-detained-report
[2] Susanto E, Adi G and Maryanto M 2018 Criminal Liability for Using Fake Letters Judging from Article 263 verse (2) of the Indonesia Criminal Code (KUHP) J. Daulat Huk. 1 1 1–12
[3] Anonymous 2017 3 tips on identifying the validity of signatures in documents [Online] Retrieved from: https://blog.bplawyers.co.id/3-Tips-Dalam-Mengidentifikasi-Keabsahan-Tanda-Tangan-Dalam-Dokumen/
[4] Blankers V L, Van Den Heuvel C E, Franke K Y and Vuurpijl L G 2009 The ICDAR 2009 signature verification competition Proceedings of the International Conference on Document Analysis and Recognition, ICDAR 1403–1407
[5] Liwicki M 2011 Signature verification competition for online and offline skilled forgeries (SigComp2011) Proceedings of the International Conference on Document Analysis and Recognition, ICDAR 1480–1484
[6] Hayatunnufus A, Andrizal A and Yendri D 2014 Detection and verification of signatures using the spatial image domain method (Universitas Andalas Padang)
[7] Sandy W K, Widodo A W and Sari Y A 2018 Determination of the authenticity of signatures using feature extraction techniques forms by the classification method of nearest neighbors and averages J. Pengemb. Teknol. Inf. dan Ilmu Komput. 2 1083–1091
[8] Senthilkumar G, Gopalakrishnan K and Satish K 2014 Embedded image capturing system using raspberry pi system Int. J. Emerg. Trends Technol. Comput. Sci. 3 2 213–215
[9] Saif J A M 2017 Tuning of Canny Image Edge Detection Int. J. Comput. Sci. Inf. Secur. 15 11 184–187
[10] Yusro M, Ramli K, Hou K M and Sudiana D 2018 Development and Performance Analysis of Canny and Hough Transform Based Pole Detection Algorithm as Mobility Aid for Visually Impaired Person on SEES (Smart Environment Explorer Stick) J. Eng. Appl. Sci. 13 7 1859–1871
[11] Islam M, Azad S U, Alam A and Hassan N 2014 Raspberry Pi and image processing based Electronic Voting Machine (EVM) Int. J. Sci. Eng. Res. 5 1 1506–1510