A Signature Comparing Android Mobile Application Utilizing Feature Extracting Algorithms

Paul Grafilon, Ian Benedict S. Aguilar, Emmanuel D. Lavarias, John Christian N. Apalin, Felnita V. Tan

Abstract: The paper presented one of the application that can be done using smartphones' camera. Nowadays, forgery is one of the most undetected crimes. With the forensic technology used today, it is still difficult for authorities to compare and define what a real signature is and what a forged signature is. A signature is a legal representation of a person. All transactions are based on a signature. Forgers may use a signature to sign illegal contracts, and withdraw from bank accounts undetected. A signature can also be forged during election periods for repeated voting. Addressing the issues, a signature should always be secure. Signature verification is a reduced problem that still poses a real challenge for researchers. The literature on signature verification is quite extensive and shows two main areas of research, off-line and on-line systems. Off-line systems deal with a static image of the signature, i.e. the result of the action of signing while on-line systems work on the dynamic process of generating the signature, i.e. the action of signing itself. The researchers have found a way to resolve the concerns. A mobile application that integrates the camera to take a picture of a signature, analyzes it, and compares it to other signatures for verification. It will exist to help citizens to be more cautious and aware with issues regarding the signatures. This might also be relevant to help organizations and institutions, such as banks and insurance companies, in verifying signatures that may avoid unwanted transactions and identity theft. Furthermore, this might help the authorities in the never ending battle against crime, especially against forgers and thieves. The project aimed to design and develop a mobile application that integrates the smartphone camera for verifying and comparing signatures for security using the best algorithm possible. As the result of the development, the said smartphone camera application is functional and reliable.

Index Terms: Forge, Forgery, Camera, Computer Vision, Smartphone

1 INTRODUCTION

"The global smartphone audience surpassed the 1 billion mark in 2012 and will total 1.75 billion in 2014", according to an article by eMarketer. It is also expected for smartphone adoption to continue on a fast-paced trajectory through 2017. Mobile phone users are rapidly switching over to smartphones as devices become more affordable and 3G and 4G networks advance [1]. With this basis, it is safe to say that smartphones are the future of mobile technology. Camera is one of the built-in features of these devices. Ranging from 2 megapixels to 41 megapixels [2], a smartphone camera is one of the many things consumers look for when buying a new unit. It is compared to DSLR cameras with its improvements in software and overall technology [3]. Primarily, the use of smartphone cameras are for taking self-portraits or "selfies", mainly for social media. This current trend limits the capabilities of a high resolution camera or even a normal 2MP camera. Mobile applications that integrate the phone camera has limited uses and almost, if not always, are used for entertainment (e.g. Retrica, Camera360). As you can see, a digital camera has many uses. A hi-res portable camera in a smartphone has countless times more. This study may determine a significant use for smartphone cameras. Forgery is one of the most undetected crimes. With the forensic technology used today, it is still difficult for authorities to compare and define what a real signature is and what a forged signature is [4]. A signature is a legal representation of a person. All transactions are based on a signature. Forgers may use a signature to sign illegal contracts, and withdraw from bank accounts undetected. A signature can also be forged during election periods for repeated voting. Addressing the issues, a signature should always be secure. Signature verification is a reduced problem that still poses a real challenge for researchers. The literature on signature verification is quite extensive and shows two main areas of research, off-line and on-line systems. Off-line systems deal with a static image of the signature, i.e. the result of the action of signing while on-line systems work on the dynamic process of generating the signature, i.e. the action of signing itself. The researchers have found a way to resolve the concerns. A mobile application that integrates the camera to take a picture of a signature, analyzes it, and compares it to other signatures for verification. It will exist to help citizens to be more cautious and aware with issues regarding the signatures. This might also be relevant to help organizations and institutions, such as banks and insurance companies, in verifying signatures that may avoid unwanted transactions and identity theft. Furthermore, this might help the authorities in the never ending battle against crime, especially against forgers and thieves. The project aims to design and develop a mobile application that integrates the smartphone camera for verifying and comparing signatures for security using the best algorithm possible.

Specifically, the objectives of the study are:

- To create a mobile application that uses the phone camera for a significant and reliable purpose.
- To evaluate the different strokes and weight of the signature via image analysis.
- To verify if the signature has a match in the database and determine if it is forged or not.
- To utilize an appropriate algorithm for the development of this project.

The study can help people in making them feel safe and secure about dealing with signatures. It can aid in verifying the signatures in contracts or deals. It may also benefit authorities in checking if the signature is forged. It is important to the research area on the basis that it is a new addition to mobile security. It aims to improve the past works on camera use and signature verification. The remainder of the paper is organized as follows: Related works are given in Section 2. In Section 3, the theories and concepts to be used in this study are discussed. Section 4 explains the requirements of creating and using this system. Section 5 reports the overall architecture of the proposed system, while Section 6 reports the experimental

procedures and the overall breakdown of work to be done. Finally, the references used are drawn in Section 7.

2 Related works

The following were the articles that are related to our study.

2.1 Camera-Based ID Verification by Signature Tracking

The camera-based acquisition system in this study uses computer vision techniques and estimation theory to track the position of the pen tip in the image plane. The verification algorithm compares the 2D shape of the signatures using a translation-invariant metric. The system proposed in this paper falls within the category of on-line systems since the visual tracker of handwriting captures the timing information in the generation of the signature [5]. The studies both aim to verify if a signature is forged or not. The differences are the platform used to verify the signature which is a software for Windows. The acquisition system is also on-line.

2.2 Feature extraction based DCT on dynamic signature verification

This study presents a simple and effective approach for an on-line signature verification system. First, the Discrete Cosine Transform (DCT) is performed on the time signals of the signature, and then DCT coefficients create a feature vector. The advantage of using the DCT is the ability to compactly represent an on-line signature using a fixed number of coefficients, which leads to fast matching algorithms. More importantly, the fixed-length is better suited, or even necessary, in certain applications related to information theory and biometric systems. Finally, several classifiers are adopted for the classification task [6]. A similarity between the proposed study and this work is the algorithms to be used, creating feature vectors.

2.3 Offline Signature Verification Using Graph Matching

In this paper, we present a simple and effective signature verification method that depends only on the raw binary pixel intensities and avoids using complex sets of features. The method looks at the signature verification problem as a graph matching problem. The method is tested using genuine and forgery signatures produced by five subjects. An equal error rate of 26.7% and 5.6% was achieved for skilled and random forgeries, respectively. A positive property of our algorithm is that the false acceptance rate of random forgeries vanishes at the point of equal false rejection and skilled forgery false acceptance rates. Keeping the normalization size at 32 × 64 pixels makes the verification time in the two seconds range [7]. The main difference of this study is the method used that will compare the two signatures. This study used a graph technique. The similarity is the signature verification being done offline.

2.4 Signature Verification on Handheld Devices

Signature verification for handheld devices (e.g. smartphones, PDAs, etc.) as an authentication method is studied. Signature can be used to authenticate users in mobile networks for secure transactions. The challenges of signature verification on mobile devices are addressed and analyzed and the architecture for a verification platform is outlined. This study proposes a verification system adapted to handheld devices and study its performance. Results are given for the scenarios of casual and skilled impostors using a subcorpus of the BIOSECURE multimodal biometric database [8]. The concept is similar to the proposed study at hand, in which a signature verification is integrated on mobile devices. However, the problem is the platform used. This study used old gen mobile devices with writing-enabled touchscreens for on-line writing.

2.5 Dynamic Signature Verification System Design Using Stroke Based Feature Extraction Algorithm

Dynamic signature verification (DSV) uses the behavioral biometrics of a hand-written signature to confirm the identity of a computer user. This thesis presents a novel stroke-based algorithm for DSV. After individual strokes are identified, a significant stroke is discriminated by the maximum correlation with respect to the reference signatures. Between each pair of signatures, the local correlation comparisons are computed between portions of the pressure and velocity signals using segment alignment by elastic matching [9]. The differences of this study are the algorithm and procedure used, which is stroke-based intended for on-line systems, and the platform.

2.6 Signature Verification for Access Control

Access control to sensitive information is a vital concern for Department of Defense agencies. Current methods employed to control access are vulnerable to unauthorized users and frequently inadequate. The use of biometric access control devices, such as signature verification systems, may represent a solution to the access control problem. This thesis looked at two dynamic signature verification systems and compared their performance in general as well as under the different operating conditions of lined and unlined paper and morning and afternoon use. The two signature verification systems were the CIC system and the Sign/On system. Additionally, the thesis compared the CIC system under both sets of operating conditions using an inking stylus pen and a non-inking stylus pen [10]. This study was created in 1991, when technology is just emerging and the verification is being argued if the pen to be used is inked or non-inked. This is related to the study at hand on the basis that it is one of the origins of signature verification via computer technology.

2.7 A Computer Vision Based Barcode System

The study focuses on barcode recognition from images of barcode stamped products, acquired by different cameras. First step in recognition of barcode data is achieving barcode localization. For this purpose, a Fast Hough Transform Approximation has been developed. With this method, barcode localization and the angular orientation of the barcode is obtained. In order to decipher barcode data, the scan line obtained by barcode localization and angular orientation information are used. However, the image resolution has to be good enough so that the bar code data could be read properly. In this work, image quality is improved with methods of B-Spline Smoothing and super-resolution techniques. Later, barcode data is deciphered via match filtering. The proposed barcode reading system is tested and results are discussed [11]. Similarities concerning the concept of recognizing a print through camera and analysis of the image is comparable. On the other hand, the object to be determined in this study are barcodes.

2.8 Signature Verification using a "Siamese" Time Delay Neural Network

This paper describes an algorithm for verification of signatures written on a pen-input tablet. The algorithm is based on a novel, artificial neural network, called a "Siamese" neural network. This network consists of two identical sub-networks joined at their outputs. During training the two sub-networks extract features from two signatures, while the joining neuron measures the distance between the two feature vectors. Verification consists of comparing an extracted feature vector with a stored feature vector for the signer. Signatures closer to this stored representation than a chosen threshold are accepted, all other signatures are rejected as forgeries [12]. Dissimilarities concerning this study are the algorithm used. It was also published in 1994, therefore its ways are already outdated and improved.

2.9 Improved offline signature verification scheme using feature point extraction method

In the paper a novel offline signature verification scheme has been proposed. The scheme is based on selecting 60 feature points from the geometric centre of the signature and compares them with the already trained feature points. The classification of the feature points utilizes statistical parameters like mean and variance. The suggested scheme discriminates between two types of originals and forged signatures. The method takes care of skill, simple and random forgeries. The objective of the work is to reduce the two vital parameters False Acceptance Rate (FAR) and False Rejection Rate (FRR) normally used in any signature verification scheme. In the end comparative analysis has been made with standard existing schemes [13]. Like the study being proposed, the scheme used in this paper is off-line signature verification. It also uses feature extraction methods. However, the difference is the platform.

2.10 An evaluation on offline signature verification using artificial neural network approach

The signature verification is the oldest security technique to verify the identification of persons. Recently, the signature recognition schemes are growing in the world of security technology. It offers two different types of schemes those are offline and online method. The offline technique means to verify a signature written on paper which is scanned to convert it into a digital image, whereas the online system required an online device such as Tablet PC, touch screen monitor by a pressure sensitive pen to verify the signature. This paper discusses a review of offline signature verification schemes which considered as a highly secured technique to recognize the genuine person's identity. It addresses the offline signature verification technique using Artificial Neural Network (ANN) approach. It also explains the fundamental characteristics of offline signature verification processes and highlights the comparison among various offline signature verification approaches and various signature recognition issues [14]. This study uses ANN, unlike the proposed system that will use feature extraction techniques.

3 THEORETICAL FRAMEWORK

This chapter contains collection of interrelated concepts or theory whereas the researchers discuss the algorithmic principles and theory used to develop the system.

3.1 Feature Extraction

The study will incorporate feature detection techniques and image extraction for the development of the application.

3.1.1 Scale-Invariant Feature Transform

SIFT, or scale-invariant feature transform, is an algorithm in computer vision to detect and describe local features in images. It was published by David Lowe in 1999. The model is chosen on the basis of computer vision techniques and image matching detection.

Figure 1. *Example of SIFT image detection*

Lowe's method for image feature generation transforms an image into a large collection of feature vectors, each of which is invariant to image translation, scaling, and rotation, partially invariant to illumination changes and robust to local geometric distortion. The figure above shows the matching key points of both images.

DoG image $D(x,y,\sigma)$ is given by

$$D(x,y,\sigma) = L(x,y,k_i\sigma) - L(x,y,k_j\sigma),$$

where $L(x,y,k\sigma)$ is the convolution of the original image $I(x,y)$ with the Gaussian blur $G(x,y,k\sigma)$ at scale $k\sigma$, i.e.,

$$L(x,y,k\sigma) = G(x,y,k\sigma) * I(x,y)$$

Figure 2. *The algorithm for SIFT*

3.1.2 Speeded Up Robust Features

SURF, or speeded up robust features, is a robust local feature detector, first presented by Herbert Bay et al. in 2006, that can be used in computer vision tasks like object recognition or 3D reconstruction. It is partly inspired by the SIFT descriptor. The standard version of SURF is several times faster than SIFT and claimed by its authors to be more robust against different image transformations than SIFT.

Figure 3. *Example of SURF keypoints on a palm*

SURF is relatively faster than SIFT in overall processing, especially in mobile programming. However, SIFT provides more attention to detail. For the application, the researchers will attempt to merge the algorithms to provide a faster but reliable matches.

Match Percentage Algorithm

For the results of the comparison, the researchers created a simple percentage algorithm utilizing feature extraction key point matches.

$$\text{PERCENTAGE} = \frac{\text{MATCHED KEYPOINTS}}{\text{TOTAL KEYPOINTS}} \times 100\%$$

$$\text{PERCENTAGE} = \frac{\text{MATCHED KEYPOINTS}}{\text{TOTAL KEYPOINTS}} \times 100\%$$

Figure 4. *Created Algorithm for comparison*

wherein total key points is image 1's keypoints + image 2's keypoints / 2.

This algorithm will also be used in determining the possibility of the signature being forged. The specifics will be provided in the next subsection, but one decision the researchers did is if the percentage of match is 96% and above, then the possibility of forgery is high.

Forgery Detection

The study will integrate principles from forensic experts for detecting forged signatures.

Shaky Handwriting

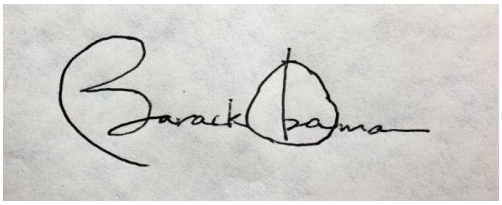

Figure 5. *An example of a forged signature with shaky writing*

The figure shows a forged signature of US President Barack Obama. Notice the shaky writing of the turns of the 'B' and the prominent shakes of the 'O'.

Letter Proportions

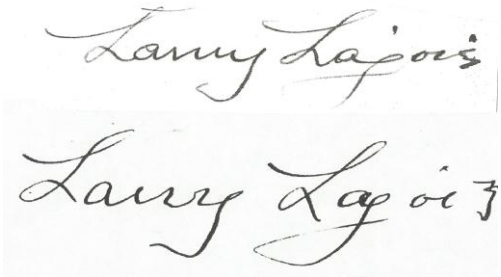

Figure 6. *An example of a forged signature comparison with the original.*

The figure shows an example of detecting forgery using letter proportions. In the lower signature, dissimilarities in the writing of small letter 'a' are mostly seen. Clear signs of forgery are also grasped in other letters, such as letter 'L' and 'y'.

Signs of Retouching

Figure 7. *An example of signature retouching*

The two signatures above are forged from the one at the lower left side of the image. The second try of forging the signature fails because of the signs of retouching in the 't' and the 'K'. Letter proportions are also shown on the last letter indicated by the arrows.

Overall Look

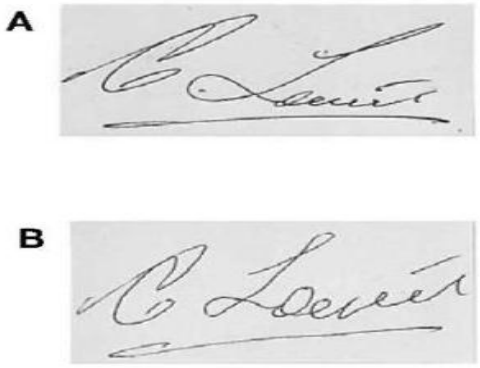

Figure 8. *A comparison of original and forged signature*

In the figure, image A shows the original signature while image B shows a forged signature. Analysis of the images shows a difference on the overall look of the signature.

Very Close Similarity

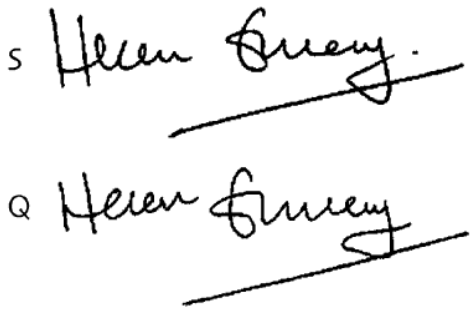

Figure 9. *An example of an almost perfect forgery*

In the figure above, the two signatures are almost exactly identical. In normal circumstances, the forged signature (image Q) would pass as an authentic signature. Forensic experts have cautioned that perfect copies of signatures have a high tendency of forgery. This is on the basis that a person has a small chance of replicating his/her signature [15].

4 COMPUTING REQUIREMENTS

This chapter contains software and hardware requirements and the system of implementation description that the researchers used for development.

4.1 Project Scope

The mobile application is for Android with a minimum version of 4.1 (Jellybean) and a 4MP camera. The app will only take pictures of the signatures, and will not include screen signing. The following are the features of the application:

- User Profile
  This is the registration section wherein user info is to be input. The user will also be required to capture his/her signature as the first image to be stored in the database.
- Image Database
  A record of all the images of signatures with a name tag for profiling. Delete option is available.
- Signature Comparison and Verification
  Once an image is taken, the application will proceed to compare and verify if the signature is in the database or not, and will advance to name 3 most possible matches in the database (via percentage breakdown).
- Forgery Indication
  After verification, if one or more of the possible matches exceeds 50%, the application will also determine the possibility of the signature being forged (also in percentage form).
- Save Signature
  The application has the option to save a signature if the percentage breakdown of the comparison to database images is under 40%.

4.2 Target User

The main target user for this project are adult individuals starting from 18 year olds who have work or currently studying. Other target users are institutions that may use this app for signature verification.

4.3 Development Tools

The project tool to be used for programming is Eclipse, operating on Windows, with ADT plugin. Android Development Tools (ADT) is a plugin for the Eclipse IDE that is designed to give you an integrated environment in which to build Android applications. Other tools used in the development of the system are Adobe Photoshop for designing and Microsoft Office for documentation and reports.

4.4 System Architecture

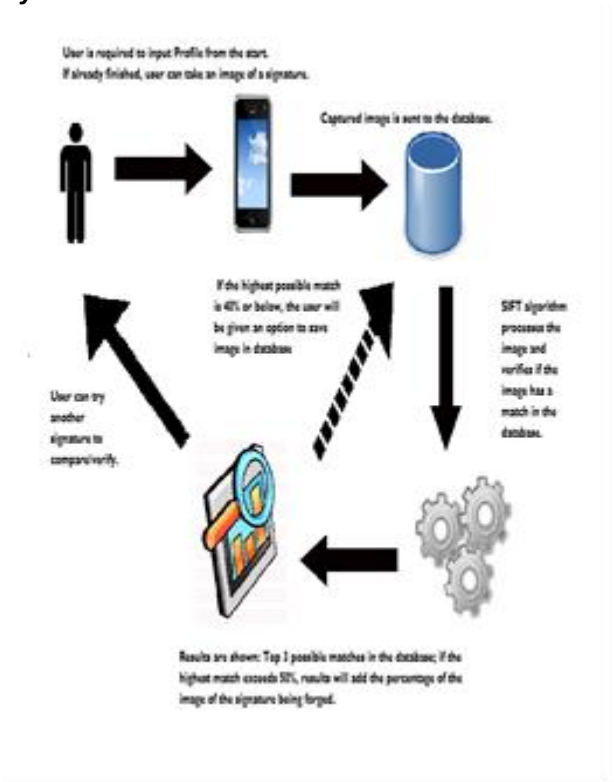

Figure 8. *System Architecture*

The figure shows the steps on how the application processes from input to output. After installation, the user inputs the profile. After this, the user can capture an image of signature. The photo is then sent to the database. The algorithm will proceed to process the image and will verify if the image has a match in the database. The output will be shown after processing. Results will include the top 3 possible matches in the database (values are in percentage form). If the highest match exceeds 50% possibility, results will add the possibility of the captured image being forged (also in percentage form). If the highest match is below 40%, the user will be given the option to save the image in the database as a new signature.

5 CONCLUSION

After the development and testing phase of this project, all algorithms, application software mentioned and applied above are interoperable, functional and reliable.

ACKNOWLEDGMENT

The authors wish to thank Paul Grafilon and Felnita V. Tan. This work was completed for the subject “IT Capstone Project” .

REFERENCES

[1]. eMarketer, 2014. Smartphone Users Worldwide Will Total 1.75 Billion in 2014. http://www.emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536

[2]. Forbes, 2013. Nokia Goes For Camera Phone Crown With 41-Megapixel Lumia - But Will Consumers Care? http://www.forbes.com/sites/parmyolson/2013/07/11/nokia-goes-for-camera-phone-crown-with-41-megapixel-lumia-but-will-consumers-care/

[3]. Yahoo! News, 2014. Smartphone cameras step closer to DSLR cameras. http://news.yahoo.com/smartphone-cameras-step-closer-dslr-cameras-071830523--finance.html

[4]. About.com, 2009. New Technique Helps Police Bust Forgers. http://crime.about.com/od/forensics/a/forgery_3d.htm

[5]. M. E. Munich and P. Perona, "Camera-Based ID Verification by Signature Tracking", in Proceedings of the 5th European Conference on Computer Vision EECV'98 (pages: 782-796), Freiburg, Germany, June 1998.

[6]. S. Rashidi, A. Fallah,, F. Towhidkhah, "Feature extraction based DCT on dynamic signature verification," Sharif University of Technology, p. 1

[7]. Ibrahim S. I. Abuhaiba, “Offline Signature Verification Using Graph Matching”, Turk J Elec Engin, VOL.15, NO.1 2007, pp. 89-90

[8]. M. Martinez-Diaz, J. Fierrez, J. Galbally, F. Alonso-Fernandez, J. Ortega-Garcia, “Signature Verification on Handheld Devices”, Biometric Recognition Group - ATVS, EPS - Univ. Autonoma de Madrid, p.1

[9]. Tong Qu, “Dynamic Signature Verification System Design Using Stroke Based Feature Extraction Algorithm”, University of Ottawa, 2004, p. v

[10]. Susan Carol Geshan, “Signature Verification for Access Control”, Naval Postgraduate School, Monterey, California, 1991, p. iii

[11]. I.S. Mehmet, “A Computer Vision Based Barcode System”, The Graduate School of Natural and Applied Sciences of Atilim University, August 2008, p. iv

[12]. J. Bromley, I. Guyon, Y. LeCun, E. Sickinger and R. Shah, “Signature Verification using a "Siamese" Time Delay Neural Network”, AT&T Bell Laboratories, Holmdel, N J 07733, 1994, p. 737

[13]. B. Majhi, Y. S. Reddy, D P. Babu, "Novel Features for Off-line Signature Verification" International Journal of Computers, Communications & Control, Vol. I, No. 1, pp. 17-24, 2006.

[14]. Prasad, A.G., and V.M.Amaresh."An Offline Signature Verification System." In IEEE International Conference on Signal and Image Processing Applications, pp.59-64.2009.

[15]. Jackson, Andrew R. W. (2007). Forensic Science. Pearson Education. pp. 235–238.