

Online Signature Verification on Mobile Devices

Miss. Hude. Kalyani. A.
Department of Computer Engineering
SCSCOE, Rahuri Factory

Miss. Khande Varsharani S.
Department of Computer Engineering
SCSCOE, Rahuri Factory

Miss. Walunj Pratiksha R.
Department of Computer Engineering
SCSCOE, Rahuri Factory

Miss. Sonawane Sonali B.
Department of Computer Engineering
SCSCOE, Rahuri Factory

Prof. Jadhav Hemant B.
Department of Computer Engineering
SCSCOE, Rahuri Factory

Abstract

In this paper the online systems explain the significances and represent the different approaches of the online signature verification. It is a simple and effective method for signature verification. An online signature is represented with different feature extractor can be applied on it. The templates of the signature are compact and require constant space. The database can be stored using the MCYT-100 database. On the signature different operations can be done they are grayscale, threshold thinning, boundary detection. The result shows the greater performance than the previous existing system it's simple and efficient. To test the system, the signature with existing template. The result demonstrates the simple online signature verification.

Keywords: online signature, mobile device authentication templating, feature extraction, reorganization verification

I. INTRODUCTION

The handwritten signature can be socially and legally accepted in the biometric trait. The signature is used for the person's identity verification. Everyone's signature is not similar. If the people having same name but they have different signature. This uniqueness of the signature can be taken as advantage in the various fields to recognize the identity of the person. The applications of signature verification are needed in such way as banking, insurance healthcare, Document management, ID security, e-commerce.

The signature verification systems can be classified into the two types i.e. the offline verification system and the on-line signature verification system. In the offline system just an image of the signature which is required for verification. It cannot require any additional attributes of the signature for the verification of the signature. So the forger who gets the images of signature can misuse the signature. It has less security provided in off-line signature. On the other hand, the online signatures have the dynamic features for the verification and give more accurate results than the offline verification system. An online system the RGB can be separated of user signature and additional attributes like grayscale, thresholding, thinning. The online signature verification are better accurate than the offline system.

It has been directed as the context of the authentication on the mobile device. There are different from are acquired from the mobile device in dynamic environment. In mobile device the user perform a signature in various way such as sitting or standing, pen up-down, mobile or immobile. Signature on the mobile device are drawn using finger resulting in less precise signals. An example of signature drawn by finger is acquired from the mobile device in fig.

This paper proposed an on-line signature verification algorithm are deploy on mobile device. It is space efficient and the computational algorithm for verifying signature. In that the signature can be stored in template in irreversible format. Then proposed method are evaluated on the public dataset and the new dataset are collected in user mobile device.



Fig. 1: An example of signatures on mobile devices.

In verification signature analysis requires no invasive measurement and people are also use in signature in daily life. Signature are generally recognized as an individual's identity by administered.

II. PREVIOUS WORK

L.G.plamondon and R. plamondon "Automatic signature verification and writer identification- the state of art" In that the state of skill in automatic signature verification can also present. It deals with most valuable result obtained and highlight of most useful direction of research. The assessment of biometric result is depends on specific application It not involve the technical issue but also social & cultural aspect. Therefore the complex theory has been proposed to model underlying the handwritten and ink-depository process, The signature verification remains open challenges to signature is judged to be genuine or forgery only on basis few refrence. [2]

D. Guru and H. Prakash "online signature verification and recognition: An approach based on symbolic representation": In this paper the most commonly used feature are signature height and width. Inthat two algorithm mostly used min algorithm and max algorithm. In this system we propose new approach for off-line signature verification is based on scored level fusion of distance &orientation feature of cendroids. In several algorithms are tested in MCYT dataset. In this work the distance between geometric cendroid &corresponding orientationandthe geometric cendroid used for bi-interval symbolic representation. Then method of signature verification based on bi-interval value symbolic representation is also proposed.[3]

Julian Fierrez , Javier Ortega-Garcia, Daniel Ramos,Joaquin Gonzalez-Rodriguez "HMM-Based On-Line Signature Verification : Feature Extraction and Signature Modeling" :The system uses a set of time sequence & hidden morkov model(HMM). Using the MCYT biomal biometric database the development & evaluation experiments are reported on a subcorpusComplaining 7000 signature from the 145 subjects. The system can be compared to other state of the art system results. A number of practical for finding related to the feature extracting & modeling in first international signature verification competition. In that only the HMM model can be used for verification. [4]

Enrique ArgonesRúa, EmanueleMaiorana, Jose Luis Alba Castro,andPatrizioCampisi Biometric Template Protection Using Universal Background Models: An Application to Online Signature : In real life application data security & privacy are crucial issues to be addressed for assuming a successful deployment of the biometrics based recognition. In that the template protection scheme exploiting the properties of eigen user space, universal background model. In that security & information leakage of the template is given. The result evaluated on the MCYT signature dataset. It can be used for biometric data. [5]

In human life security takes important role. Nowadays it is the basic fundamental of all system developed. For this purpose, biometric authentication system got a lot of importance . Biometric system is secure, easy to use, and easy to develop. Among these techniques signature verification is the most secure or famous one because of cheap data acquisition devices.[6] We use the on-line –signature verification in every kind of real time applications such as credit card transactions, banking system, colleges, Hospitals etc.

III. ONLINE SIGNATURE VERIFICATION ALGORITHM

1) Image processing

What is an image?

An image is an array, or a matrix, of square pixels (picture elements) arranged in columns and rows.

In greyscale image each picture element has an assigned intensity that ranges from 0 to 255. A grey scale image is people normally call a black and white image. An image will also include many shades of grey.

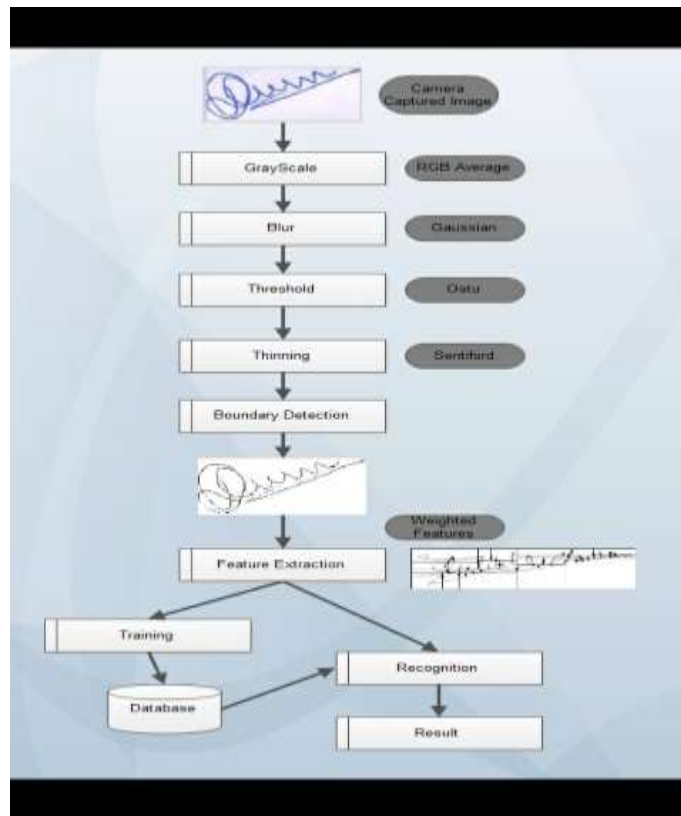


Fig. 1: Architecture of signature verification

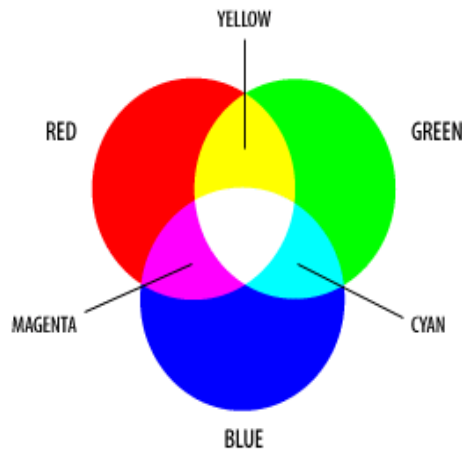
IV. COLOURS

For the science communication, the two main colour are RGB and CMYK is important.

A. RGB:

The RGB colour model relates is very closely to the way we perceive colour with the **r**, **g** and **b** receptors in our retinas. RGB uses additive colour mixing and it is the basic colour model used in television or any other medium that projects colour with the light. It is basic colour model used in the computers and for web graphics, but it cannot used for the print production.

The secondary colours of the RGB – cyan, magenta, and yellow – are formed by mixing two of the primary colours such as red, green or blue and excluding in the third colour. Red and green combine to make the yellow, green and blue to make cyan, and blue and red form magenta. The combination of red, green, and blue in full intensity makes white.



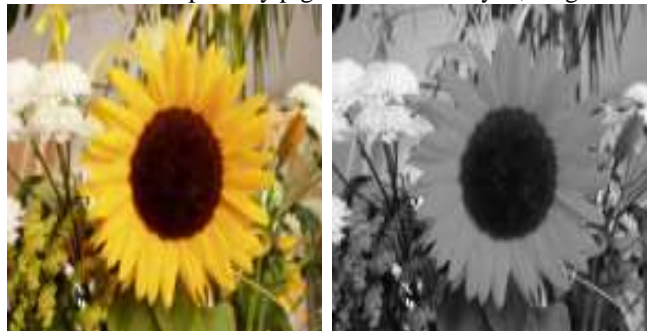
In a Photoshop using the “screen” mode for the different layers in an image will make the intensities mix together it according to the additive colour mix model. This is analogous to the stacking slide images on top of each other and shining light through them.

B. Grayscale Image:

A grayscale is the digital image is an image in which the value of each pixel is the single sample, it carries only intensity information but the no chromatic information. They are composed in exclusively of the shades of the gray varying from the black as the weakest intensity and the white as the strongest. These images are also called as black image and white images. It is also known as binary image. It is to be noted however that the term black image and white image is the description is something of a misnomer because in addition to black and white, they consist of varying the shades of gray.

Grayscale images are distinct from one-bit the black and the white images, In which the context of computer imaging are images with only the two colors, black and white (are also called bi-level or binary images). The single bit black-and white images are called as binary images. The standard grayscale images are actually eight bit black-and-white images such, in that pixel there is a set permissible values. Due to this, the grayscale images have many shades of gray in between. The reason for the separation of these images from any other sort of colour images is that less information needs to be provided for the each pixel. Gray colour is the one in which all the red, green and blue components have equal intensities. So that it is so necessary to the specify only a single intensity value for each pixel.

The intensity of a pixel is expressed within the given domain of 28 values between a minimum and a maximum, additionally. This range can be represented is an abstract way as a range from the 0 means total absence of black and 1 means total presence of white, with any fractional values in between. The darkest possible shade is black, and which is the total absence of the transmitted or reflected light. The lightest possible shade is the white, the total transmission or reflection of the light at all visible wavelengths. The intermediate shades of gray are represented by the equal brightness levels of the three primary colors (red, green and blue) for transmitted light, or the equal amounts of the three primary pigments such as cyan, magenta and yellow for reflected light.



Before

After

C. Blur Image:

1) Definition

The image terms blurring means that each pixel in the source image gets spread over and mixed into the surrounding pixels.

- Another way to look at this is that each pixel in the destination image is made up of out of a mixture of surrounding pixels from the source image.



ORIGINAL IMAGE



BLURRED IMAGE

Why should we create the Blurred Image?

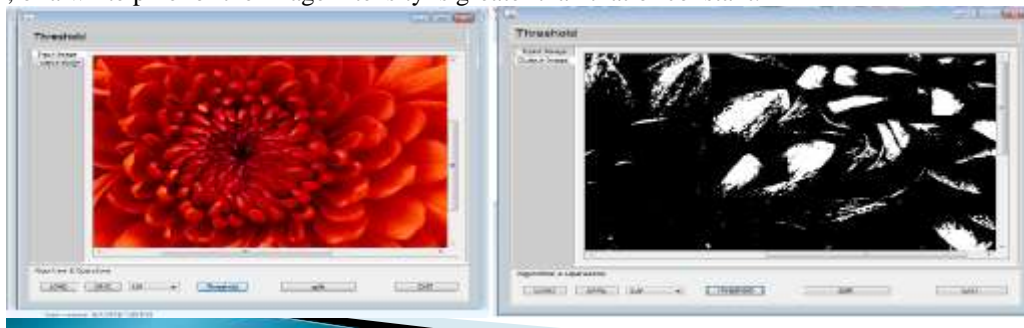
- The blurring image can reduces the sharpening effect, this makes the detection more accurate.
- There are two type of blurring an image
 - Gray scaled blur.
 - Colour blur.

How do we Blur an image?

- Steps or Algorithm
- Traverse through the entire input image array.
- The read individual pixel colour value (24-bit).
- Split the colour value into separately such as R, G and B 8-bit values.
- In Calculate the RGB average of surrounding pixel sand assign the average value to it.
- Repeat the above required step for each pixel.
- Store the new value at the same location in output image.

2) Thresholding:

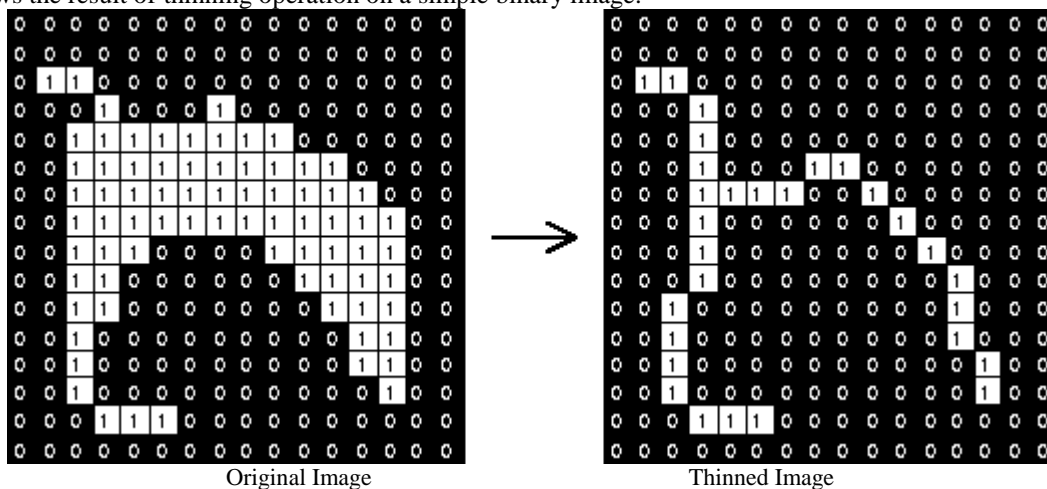
It is the simplest method of image segmentation. Form a grayscale image, thresholding is used to create binary image. The simplest thresholding method replace each pixel in an image with a black pixel if the image intensity is $I_{i,j}$ less than the sum fixed constant T, or a white pixel of the image intensity is greater than that of constant.



D. Thinning

1) Thinning Algorithm:

Thinning algorithm is a Morphological operation that is used to remove the selected foreground pixels from the binary images. It preserves the topology (extent and connectivity) of the original region while throwing away all of the original foreground pixels. Figure 1.1 shows the result of thinning operation on a simple binary image.



Thinning is somewhat like erosion or opening. It can be used for the several applications, but it is more particularly useful for the skeletonizing and Medial Axis Transform. In this model it is commonly used for tidy up the output of edge detectors by reducing all lines to the single pixel thickness.

The morphological operators, thinning operators take into two pieces of data as the input. One is the input image, which is may be either binary or greyscale. The other is that structuring element, which are determines the precise details of the effect of the operator on the image.

V. BOUNDARY DETECTION

Boundary detection in range images.

The great importance of boundary or edge detection is an early stage for more complicated image processing or computer vision task is the known since many years. The image segmentation technique fails to provide the accurate information about the shape and the position of the object in the image. Edge detection can accurately determine the object boundaries which are closely related

to the shape and the position of the object. So that boundary detection complements image segmentation. Edge detection in range images is one of the most essential component of the overall strategy. Edge detection is used as the preprocessing stage. Render the task of edge detection image are more elaborate than edge detection in intensity images.

VI. CONCLUSION

This paper proposes a simple and effective method for online signature verification system is suitable for the user authentications on a mobile device. An image processing is the study of representation and manipulation of the pictorial information. Digital image processing is performed on digital computer that manipulate the images as arrays or matrices of numbers. The conversion of an image to a lower bit grayscale does not require an encoding technique. The basic conversions are only displayed. Blurring image reduces the sharpening effect that makes the detection more accurate. It is the simplest method of an image segmentation. Form a grayscale image, thresholding is used to create binary image. Thinning used to remove selected foreground pixels from binary images. Users can encode the images to their preferred encoding technique. However, it is quite obvious that smaller the number of bits used, the image quality will be degraded. When thinning is complete, there are still pixels that could be deleted (principal of among these are pixels that form a staircase). It is possible to use Holt's staircase removal algorithm, which allows half of the pixels in a staircase to be removed without the affecting the shape of connectedness of the overall object by applying a template-matching technique. The security of system can be increase.

REFERENCES

- [1] Napa Sae-Bae and NasirMemon, Fellow, IEEE "Online signature verification on mobile device" IEEE transaction on information forensic and security, vol. 9, no. 6, june 2014
- [2] L. G. Plamondon and R. Plamondon, "Automatic signature verification and writer identification—The state of the art," *Pattern Recognit.*, vol. 22, no. 2, pp. 107–131, 1989.
- [3] D. Guru and H. Prakash, "Online signature verification and recognition: An approach based on symbolic representation," *IEEE Trans. PatternAnal. Mach. Intell.*, vol. 31, no. 6, pp. 1059–1073, Jun. 2009.
- [4] J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez-Rodriguez, "HMM-based on-line signature verification: Feature extraction and signature modeling," *Pattern Recognit. Lett.*, vol. 28, pp. 2325–2334, Dec. 2007.
- [5] E. ArgonesRua, E. Maiorana, J. Alba Castro, and P. Campisi, "Biometric template protection using universal background models: An application to online signature," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 269–282, Feb. 2012.
- [6] H. Feng and C. C. Wah, "Online signature verification using a new extreme points warping technique," *Pattern Recognit. Lett.*, vol. 24, no. 16, pp. 2943–2951, 2003.
- [7] N. Sae-Bae and N. Memon, "A simple and effective method for online signature verification," in *Proc. Int. Conf. BIOSIG*, 2013, pp. 1–12.
- [8] N. Seabee, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: A novel approach to authentication on multi-touch devices,"
- [9] H. Feng and C. C. Wah, "Online signature verification using a new extreme points warping technique," *Pattern Recognit. Lett.*, vol. 24, no. 16, pp. 2943–2951, 2003.
- [10] M. Faundez-Zanuy, "On-line signature recognition based on VQ-DTW," *Pattern Recognit.*, vol. 40, no. 3, pp. 981–992, 2007
- [11] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable templates for sequence-based biometrics with application to on-line signature recognition," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 40, no. 3, pp. 525–538, May 2010.