USING COMPUTATIONAL INTELLIGENCE TO VERIFY ELECTRONIC SIGNATURES

[1]MATLHOGONOLOD. MOOKI, [2]JOHNSON O.DEHINBO

[1,2]Computer Science Department, Tshwane University of Technology.South Africa
E-mail: [1]mdmooki@gmail.com, [2]Dehinbooj@tut.ac.za

Abstract - Electronic signature is not limited to only the electronic handwritten representation of a traditional pen to paper signature. According to ECTA (2002:10) electronic signature means data associated with an individual that serves as a signature which includes biometrics data (fingerprints, retina scans, facial scan). ECTA has laws that have specific requirements for an electronic signature and electronic representation of a signature which is the focus of this research meets the requirements. Electronic signatures as attested by [4] form a capability to allow two parties online to have agreement which is binding by law. In this paper, we look at a way to verify electronic signatures by comparing two electronic signatures of an individual. The focus will be on comparing between a face-to-face signature we have on a database and the new captured signature on a canvas online. To improve the acceptability of signature authentication standards we will be doing a comparison that will calculate the accuracy of two handwritten electronic signatures and return a percentage that will confirm if the electronic signature is from the same individual or not, which will make electronic signature secure and accurate to a specific individual.

Keywords - Computational Intelligence, Signature comparisons, Signature verifications, SignatureAuthentication Standards.

I. INTRODUCTION

According to the law dictionary [6] a signature represents the acceptance, approval or obligation to an agreement. As observed by [8] handwritten signatures are the most trusted methods for agreements between one or more parties today and have been for a long time, however the limitation with handwritten signatures as mentioned by [10] is that they need face to face interaction. Digitizing and verifying this already widely used method can put a lot of people at ease and as [12] points out it can also play an important role in authenticate and authorizing legal transactions. Electronic signatures have already been proven to be faster and cost effective for two people to reach a binding agreement. Electronic signatures refer to any data that can identify an individual online.

1.1. Background of the Research Problem

Currently there are systems that use handwritten electronic signature, with limitation of verifying if the signature belongs to the intended owner. In this paper, we focus on verifying user electronic signature without the limitations of hardware.

The verification can be done after a signature has been successfully captured on any touch screen devices, such as notepads, touch laptops, phones (any smart phone). In all simplicity, the first signature is captured on a face to face process, where there's surety that the signature belongs to an individual. Once the first signature is captured a user can capture a signature from anywhere and that signature will be compared to the existing signature using a percentage to calculate the accuracy. The limitation of this will be the first capturing of the signature as it will require the user to be in a face to face situation.

1.2. The Problem Statement

Having an agreement with a user online can be a problem if the user is not verified. For institutions to protect their users and themselves, it is crucial for them to verify if the user is who he/she says he/she is, as verification is a vital tool for confirming user identity.

The main problem we are solving is verifying a user through a handwritten electronic signature by comparing an existing signature to the captured signature. This paper does not address the security issues of electronic signature although [15] addresses it by informing us of the standards accepted methods of authenticating digital documents by using digital certificates.

We will only be focusing on comparing the handwritten electronic signature assuming the entire digital standards are met. In terms of electronic signature, we will only be focusing on verifying handwritten electronic signature, and this does not include verifying using public keys and private keys as explained by [7].

1.3. The goal of the Research

This paper is not aimed at replacing HSV systems that exists but to improve the results of HSV to produce better results, we do this by developing and designing a system that uses API's for verification of a handwritten signature online and calculates the results.

1.4. Research questions

The research questions are:

- How to improve online handwritten signature verification?
- How to authenticate a user through the verification of handwritten online signature?

1.5. Importance of the Study

Verification of a user as explain earlier is crucial for agreement to be binding between two parties and as [5] attest handwritten signatures are highly accepted for a verification of a user. This research will first verify if the signature belongs to the users in question by improving the verification of handwritten signature and furthermore this research will use that signature to authenticate the identity of the user.

II. LITERATURE REVIEW

2.1. Introduction

There's been several ways to authenticate handwriting electronic signature such as handwritten signature verification (HSV) involves online and offline verification as attested by [8], Biometric signature which imbeds information about a handwritten signature into a message and then compares the message to authenticate if it's the same to draw a conclusion about the verification. There are several reasons for verifying a signature, mostly being that the human verification cannot be trusted. Previous study [2] attests that there are three types of forgeries namely Skilled, Casual and random forgeries of which skilled forgeries has two subcategories namely professional and amateur forgeries.



Figure 1. Forgery types

An author [19] defines skilled forgeries as forgery done by a professional who has experience in copying signatures. With Skilled come profession and amateur based on how much of experience the forger has. Casual forgeries are defined by [19] as signature done by a forger in his own style without the knowledge of the spelling and no experience. Random forgeries according to [14] is when the forger has no knowledge of the shape of the genuine signature, the forger just uses the name of the victim to in his own style.

2.2. Handwritten Signature Verification (HSV)

Aprevious study [9] believes that HSV is a trusted method to identifying and verifying a user, they verify handwritten signatures using dynamic features, such as the time series of the pen's position, pressure, velocity, acceleration and elevation for verification, limitations to this sort of verification is uses hardware rather than software. There's offline HSV which takes signatures from scanned pdf file and online which uses touch screen devices such (tablets, phone etc). This research is interested on the online verification as we will only be doing verification across the network rather than paper based. According to [6] HVS uses 6 step procedures for verification namely:

1. Registration - this step refers to capturing the first signature by the user most likely on a face to face basis.
2. Pre-processing and referencing - this step refers to removal of pen-up strokes.
3. Test signature - this step is when the users capture a new signature.
4. Comparison processing - which refers to comparing two signatures based on the distance and time measurement difference to conclude it's the same.
5. Performance evaluation – this is the stage where if the compassion is different the system either accepts it or reject the difference.
6. It the repetition of step 3 to 5 for concrete results.

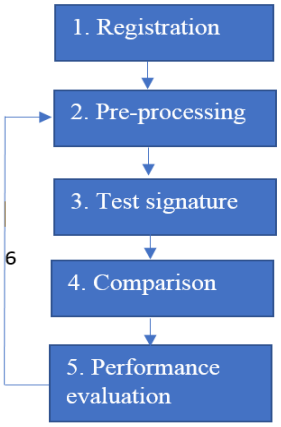


Figure 2. 6 steps procedures for verification

2.3. Biometric Signature

Biometric signatures are a representation of handwritten signature. An author [17]considers the unique characteristics of the handwritten signature based on the pressure applied, speed, and graphical representation of the pattern of the signature and they use the data gathered and assign it to a massage to verify the signature. If the message they have differs from the original message they captured the signature is considered not authentic. This type of verification takes into consideration the speed and pressure of the captured signature which this paper does not take into consideration as it is focus on the device. According to a previous author [11], biometrics has two categories namely physical biometrics that involves human body characteristics such as (retina scans, facial features, fingerprints, hand geometry, earlobe geometry and DNA) and behavioral include features about human characteristics such as the voice, handwriting etc.

2.4. Hidden Markov Model (HMM)

Another widely used model for HSV is HMM [15] explains them as a way that verifies a signature using values in vectors to determine the related points of the signature. A previous study [13]believes that the selection of set of feature vectors can lead to more effective results as they could draw the change between patterns and their similarities.

III. RESEARCH DESIGN AND METHODOLOGY

3.1. Introduction

This paper uses quantitative research approach by a developing and designing a system to authenticate the user and improve the verification of a handwritten signature online. This system is not aimed at replacing HSV systems that exists but to improve the results of HSV.

This research follows the positivism research design which employs a prototype methodology. Prototyping is used to gather the design requirement of the actual signature verification system.

The development system is for literate people as it requires you to sign your name or have a unique hand-written signature. We focus on ages 21 – 45 years old individual as they are in the age group of not changing signatures constantly. We further look for people who do not have hand shaking, tremor or neurologic disorder as that will affect the results of our research.

3.2. Prototyping

According to Mdluli & Dehinbo (2016:104) a prototype is a sample system built to investigate and determine about the process it can achieve, it is usually built to analyze newly designed functionality to increase quality of usability that involves running systems rather than focusing on theoretical level. Further information is given in the system design.

3.2.1. System tools

The web application interface is build using a web development language; HTML (Hyper-Text Markup Language) that the users access when capturing their signature online. The use of an HTML canvas is used as an element that is used to of capturing the signature. Java programming language to create a servlet that will save the captured signature to the application workspace. The application workspace will contain the temporary base64 string of the newly captured signature image that will use to do the comparison with the first originally captured signature image. The base64 string of the first originally captured image is saved to a MySQL database along with the identity number of the user.

PHP is used to convert extract the image feature of the captured signature. Python to compare between the signatures and return results, SIFT and TM_SQDIFF will be used both are OPENCV methods from Python.

3.2.2. System Architecture and flowchart

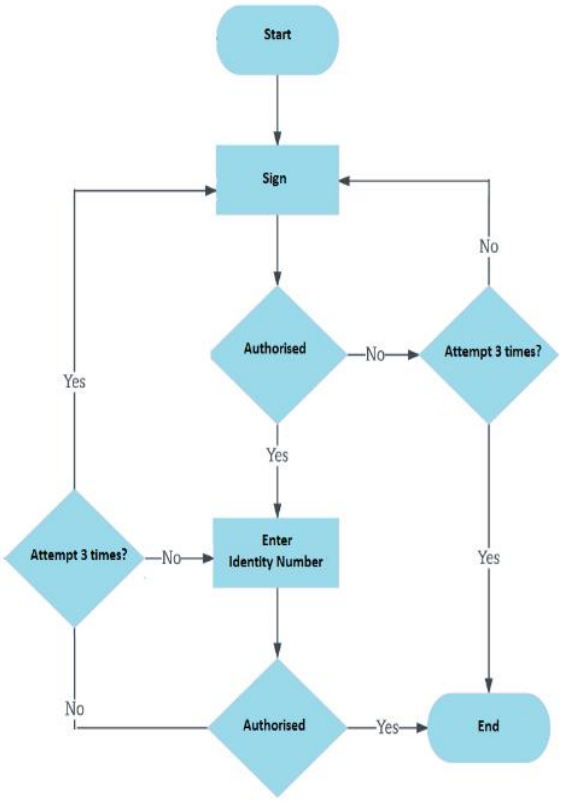


Fig.3. Weight Change as a function of cycle number YSZ TBCs during thermal fatigue testing.

3.2.3. System algorithm

This is the logic of the system. The explanation is as follows:

The user signs on a canvas
If newly captured signature compared to saved signature comparison accuracy is greater than 75%
Then
~ Users is partially verified
Else If identity number is the same as the signature verified
Then
~ Users successfully verified
Else
~ user not verified.
End if
Else
~ The user is not verified
End if

Coding and application of the algorithm would transform an example of a newly captured signature in figure 3 into an example feature extract in figure 4.

Example 1



Figure 4. Example 1 newly captured signature

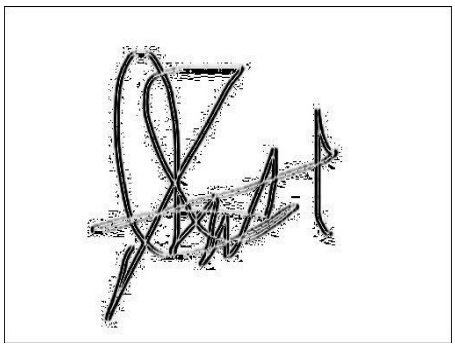


Figure 4. Example 1 newly captured signature feature extract

In the verification phase

1. Image feature extraction

To extract image feature will be using edge detection. Edge detection according to [18] is a tool used in image processing for capabilities such as feature detection and feature extraction, it achieves this by identifying image points. To achieve this, it uses a 3x3 convolution masks which estimates the y and x directional change.

Conventional mark:

$$\mathbf{G}_y = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ +1 & +2 & +1 \end{bmatrix} * \mathbf{A} \quad \text{and} \quad \mathbf{G}_x = \begin{bmatrix} -1 & 0 & +1 \\ -2 & 0 & +2 \\ -1 & 0 & +1 \end{bmatrix} * \mathbf{A}$$

Figure 10. TM_SQDIFF Compare results

Where Gy and Gx are the Gray representation estimates of the y and x directional change and A is the image.

Once the values of the Gy and Gx are established, you combine them using a formula to get the Gray representation:

$$\mathbf{G} = \sqrt{\mathbf{G}_x{}^2 + \mathbf{G}_y{}^2}$$

The extraction of feature results in a histogram creation, which makes it easy to compare two images further it also detects the pressure points in the signature.

IV. SYSTEM IMPLEMENTATION AND RESULTS

4.1. Introduction

The home page of the system has a canvas that enables the user to sign so that they can be verified. The user needs to first save the signature or clear it if they are not happy with the captured signature, after saving the signature the user then clicks Finish button to send the signature for verification.

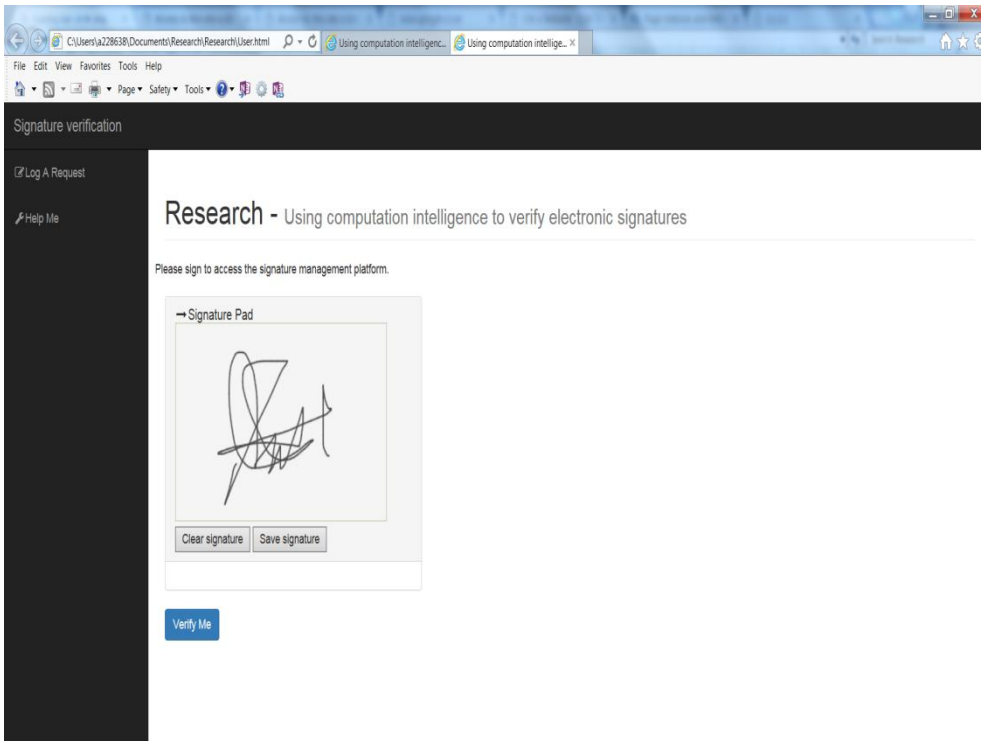


Figure 5. TM_SQDIFF Compare results

The verification is calculated by comparing the existing signature on the database to the newly captured signature. If the results are greater than 75% the user name and surname of the compared signature appears. The identity number of the user is required to confirm the user of the captured signature. If the identity number matches the identity number that is on the database and the signature belongs to the user of the entered signature. The system then opens a screen with the information of the user as the users has successfully been verified with their signature. My account tab also appears for the user to able to change any information they need to change on their user account.

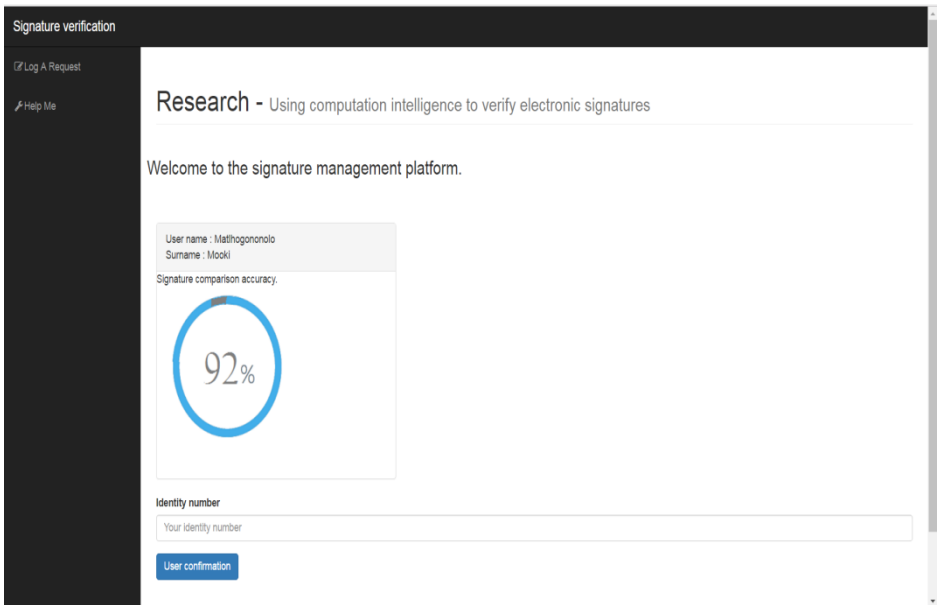


Figure 6. Verification results of the handwritten signatures

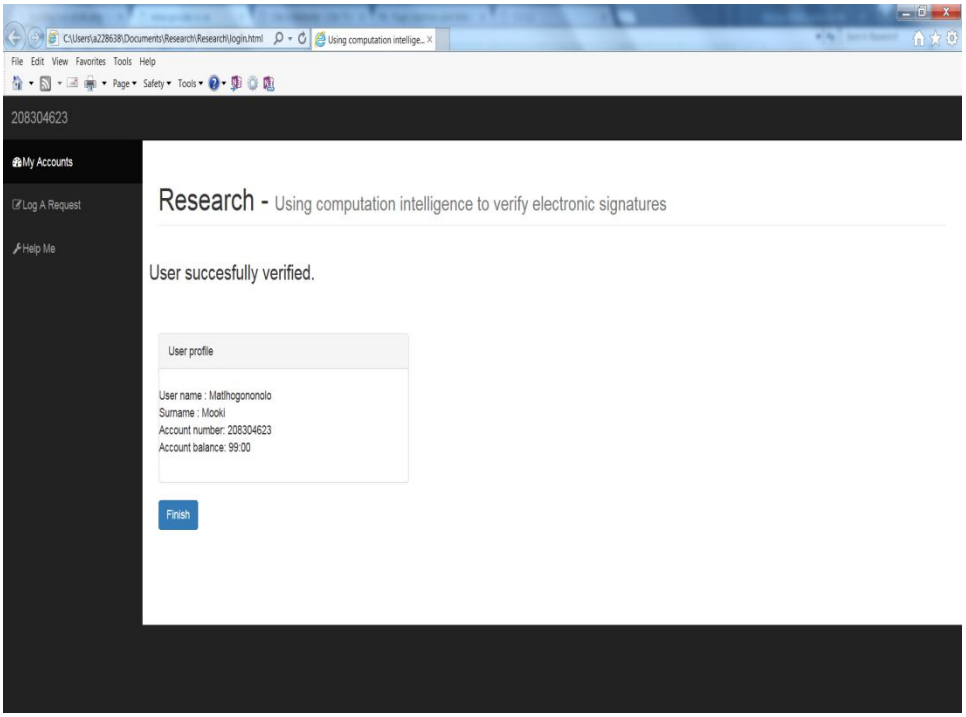


Figure 7. Profile home page of a successfully verified user

If the verification accuracy is less than 75 percent, the system will not link the signature to a user but will tell the user to try again. The user won't be prompt for their identity number but will have an option to try again. If a signature gets more than 60 percent accuracy and less than 75 percent for more than 3 times in the row on the same device, the login for that signature will be blocked as well as if the identity number is entered incorrectly three times.

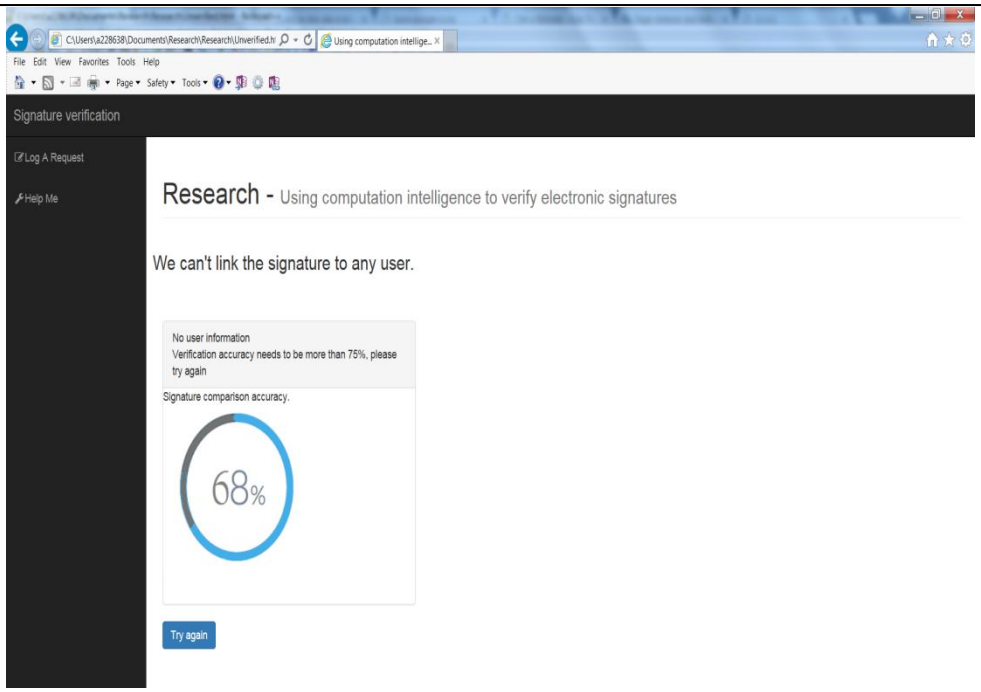


Figure 8. Accuracy less than 75 percent error page

V. CONCLUSION

This paper is aimed at using handwritten signature as an authentication mechanism to verify a user and give them access to systems, to achieve this handwritten verification must improved. Investigations on handwritten signature verification as an appealing method to login was assessed.

In consideration to security:Most user gave concerns of security not being enough in handwritten signature verification.

Python was considered as a preferred language because it uses machine language consideration, PHP was used to extract feature as it is a language I am familiar to using.

Both SIFT and TM_SQDIFF from python image classification was used, SIFT was used as it can detect similarities even if the image is rotated, and TM_SQDIFF was used to do 2D convolution, which is a template matching mechanism. Both image classifiers used are opencv classifiers that are supported on python.

A prototype was used to show the user the concept of the proposed system and how the system works. It resulted in users being able to understand what the system entails and how to use it.

REFERENCES

[1] ECTA, ELECTRONIC COMMUNKATIONS AND TRANSACTIONS ACT, 2002; https://mymobileoffice.online//documentation/ ecta.pdf (2002).

[2] P. M. D. Correia, A. B. Augusto, A. B. Augusto, the authentication of handwriting signature by using motion detection and qr code, http://www.newyorker.com/magazine/2017/01/02/rewritingthe-code-of-life (2015).

[3] N. Zheng, A. Palosk, A. Palosk, H. Wang, H. Wang, An efficient user verification system via mouse movements, http://www.cs.wm.edu/~hnw/ paper/ccs11.pdf

[4] Electronic signatures for south african law firms, http://www.lssa.org.za/upload/documents/LSSA\%20Guidelines\ Electronic\ %20Signatures\%20for\%20South\%20African\%20Law\%20Firms\ October\%202014.pdf (2014).

[5] R. Gates, M. Nuzum, M. Nuzum, H. G. Byers, H. G. Byers, H. J. Bessey, H. J. Bessey, http://www.supremecourt.ohio.gov/boards/actc/sgr/esignatures.pdf, produced by the Electronic Signatures Work Group of the Standards Subcommittee of the Supreme Court of Ohio Advisory Committee on Technology and the Courts ; http: //www.supremecourt.ohio.gov/Boards/ACTC/SGR/ESignatures.pdf (2008).

[6] Encyclopedia of american law, defination of signature; https://legaldictionary.thefreedictionary.com/signature (2008).

[7] Public key encryption and digital signature: How do they work?, https: //www.cgi.com/files/white-papers/cgi\ whpr\ 35\ pki\ e.pdf (2004). November 7, 2017

[8] S. Garhawal, N. Shukla, N. Shukla, A study on handwritten signature verification approaches, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 2 (8), http://ijarcet. org/wp-content/uploads/IJARCET-VOL-2-ISSUE-8-2497-2503.pdf.

[9] P. V. Hatkar, Z. J. Tamboli, Z. J. Tamboli, Image processing for signature verification, International Journal of Innovative Research in Computer Science & Technology (IJIRCST) 3 (3), http://www.ijircst.org/ DOC/27\ IRP366728255fa-1a7d-4123-a99b-3a4ba558ba43.pdf.

[10] J. J. Igarza, I. Goirizelaia, I. Goirizelaia, K. Espinosa, K. Espinosa, I. Hern´aez, I. Hern´aez, R. M´endez, R. M´endez, J. S´anchez, J. S´anchez, Online handwritten signature verification using hidden markov models, http://citeseerx.ist.psu.edu/viewdoc/download?doi= 10.1.1.158.2091\&rep=rep1\&type=pdf (2003).

[11] A. Dhawan, A. R. Ganesan, Handwritten signature verification, https:// www.ida.liu.se/~TDDD17/oldprojects/2009/projects/006.pdf (2017).

[12] M. Querini, M. Gattelli, M. Gattelli, V. M. Gentile, G. F. Italiano, A new system for secure handwritten signing of

documents, International Journal of Computer Science and Applications 12 (2) (2015) 37–56.
[13] S. F. A. Zaidi, S. Mohammed, Biometric handwritten signature recognition, https://www.ida.liu.se/∼TDDD17/oldprojects/2009/ projects/006.pdf (2017).
[14] T. B´alint, J. Bucko, J. Bucko, Comparative analysis of handwritten, biometric and digital signature, International Review of Social Sciences and Humanities 4 (2) (2013) 43–53, https://elifesciences.org/content/3/ e03401.
[15] A. Pansare, S. Bhatia, S. Bhatia, S. Bhatia, Handwritten signature verification using neural network, International Journal of Applied Information Systems (IJAIS) 1 (2) (2012) 1–6, http://citeseerx.ist.psu.edu/ viewdoc/download?doi=10.1.1.402.1616\&rep=rep1\&type= pdf.
[16] M. Mdluli, J. O. Dehinbo, Development of an audio-visual based e-learning system to enhance interaction between learners and teachers, Proceedings of 2nd International Conference on E-Learning Engineering and Computer Softwares (2).
[17] E. Feronato, Image edge detection algorithm – php version, http://www.emanueleferonato.com/2010/ 10/19/image-edge-detection-algorithm-php-version/.
[18] Electronic signature, https://en.wikipedia.org/wiki/Electronic_signature, (1 November 2017)
[19] Alexander Mordvintsev, Abid K, Introduction to SIFT (Scale-Invariant Feature Transform), http://opencv-python-tutroals.readthedocs.io/en/latest/py_tutorials/py_feature2d/ py_sift_intro/py_sift_intro.html, 2013

★★★