Time/Space based Biometric Handwritten Signature Verification

Ricardo P. Gonçalves, Alexandre B. Augusto, Manuel E. Correia
Department of Computer Science, Faculty of Science, University of Porto
Center for Research in Advanced Computer Systems (CRACS-INESC)
Porto, Portugal
ricar.goncalves@gmail.com, aaugusto@dcc.fc.up.pt, mcc@dcc.fc.up.pt

Abstract — **Handwritten signature recognition is still the most widely accepted method to validate paper based documents. However, in the digital world, there is no readymade way to distinguish a real handwritten signature on a scanned document from a forged copy of another signature made by the same person on another document that is simply "pasted" into the forged document. In this paper we describe how we are using the touch screen of smartphones or tablets to collect handwritten signature images and associated biometric markers derived from the motion direction of handwritten signatures that are made directly into the device touchscreen. These time base biometric markers can then be converted into signaling time waves, by using the dragging or lifting movements the user makes with a touch screen omnidirectional tip stylus, when he handwrites is signature at the device touchscreen. These time/space signaling time waves can then be converted into a biometric bit stream that can be matched with previously enrolled biometric markers of the user's handwritten signature. In this paper we contend that the collection of these simple biometric features is sufficient to achieve a level of user recognition and authentication that is sufficient for the majority of online user authentication and digital documents authenticity.**

Keywords - signature; handwriting; biometric; verification; authentication.

I. INTRODUCTION

Modern society processes are rooted on written notarized contractual documents that then act as proof of certain actions or facts about individuals or other entities that result from many societal interactions like for example enterprises or persons establishing legal binding contracts between them. These paper based documents must then be laden with security artifacts that make them hard to forge and attest about the document authenticity, integrity and the time it was produced. They often act as root proof of important facts, e.g. to proof who is the owner of a property, if some payment was made and on what circumstances, prove what the monthly income is in an employee contract, etc. Over the years society evolved some overall well-accepted procedures and security artifacts that allow one to consider these documents as authentic and acceptable in a court of law, the most common of which is the handwritten signature and the embossing institutional stamp.

Unfortunately these highly accepted societal procedures base their security on the intrinsic physical properties of the paper that is used to print and hand sign or stamp these documents. For digital documents these physical security properties of paper do not hold anymore and therefore we need to adopt other security mechanisms if one wants to be able to produce digital documents with security properties analog to what can be cheaply and easily achieved with paper. In the real world, due to the physical characteristics of paper, handwritten signatures and embossing stamps constitute privileged ways to secure and attest the integrity and authenticity of printed documents. However in the digital world, there is no readymade way to distinguish real handwritten signature on a scanned document from a forged copy of another signature made by the same person on another document that is simply "pasted" into the forged document. As soon as one paper document, with a real handwritten signature, is digitalized anyone who can access a copy can then use the digitalized handwritten signature to impersonate the signature owner in every other kinds of digital documents, by simply pasting an image of the handwritten signature into the forged document. This is why one can only safely attest on the authenticity of a handwritten signature that is made on the original physical paper document. This is rather unfortunate because this implies a waste of paper resources and the involvement of a trusted third party (a notary service) each time a copy of the original document is needed. This process is obviously quite expensive and highly inefficient.

The standard accepted method of authenticating digital documents is using digital signatures based on X509 digital certificates. This is a well-accepted legal method to secure digital documents. However, due to its technical complexities, certificate based digital signatures are still not well accepted by the general population. One as only to remember that for example a great percentage of the Portuguese population already has an identification document ("cartão do cidadão"), capable of performing legal binding digital signatures, but that almost no one uses. Culturally, at least in the western world, the general public still has more affinity and can more easily relate security with a visual analysis of handwritten signatures. This has been true historically and is still valid today [1].

Unfortunately, this imposes severe restrictions on the widespread use of digital documents as an acceptable source of proof for society business processes, thus severely limiting their applicability and use. As a result the great majority of societal processes, which require signed documents, will keep using paper documents. This makes the entire process much more expensive and slower, with enormous societal costs as a whole. Typically, the great majority of bureaucratic processes suffer from this problem.

With this work we want to start building a better bridge of confidence between the general public digital documents based whose security is based on the unique characteristic of biometric markers that can be derived from the dynamics of movement of the human hand when it performs a handwritten signature, something everyone on a western culture is trained to do. From these we can then derive security digital artifacts to include into digital documents, to attest their authenticity and security. We strong believe that security mechanisms for digital documents, based on what people are already used and trained to do, to secure paper based documents have a more chance of success and general acceptance then the more classical, but less well accepted approach of securing digital documents with the technically more challenging certificate based digital signature mechanisms.

II. ARCHITECTURE

Our proposal is based on a biometric online authentication infrastructure, which authenticates a user based on the dynamics of his hand movement when he performs a handwritten signature in the screen of a tablet or mobile phone.

To be authenticated a user will first need to be enrolled into the system. During this process, he will be asked to introduce a couple of reference handwritten signatures that will be used to build a biometric template reference that will them be used to authenticate him online. In order to refine the users template practice the user is asked to repeat his signature several times.

On Fig. 1 we can see an overview of the systems overall architecture. The enrollment procedure proceeds as follows:

- The user starts by requesting a new ID. This ID will be associated with his handwritten signature.
- The system confirms the creation of a new ID and generates a QR code based on that ID that is displayed on the screen. This QR code contains a URL that directs the mobile device browser to a canvas based HTML5 web application, where the user is invited to draw his signature. At the same time this web app collects biometric markers from the user's pen movements on the mobile phone or tablet screen.
- The user points his mobile device with a camera to the QR Code. The device decodes it and opens the web HTML5 application referenced by the QR Code.
- The signature is acquired and sent to the users enrollment server.
- The enrollment server returns feedback to client, which includes a bitmap of the drawn signature ready to be integrated into a digital document.

This work-flow can be used as means to enroll a new user's handwritten signature as well as to biometrically authenticate a user by the way he writes his signature on the mobile phone or tablet screen.

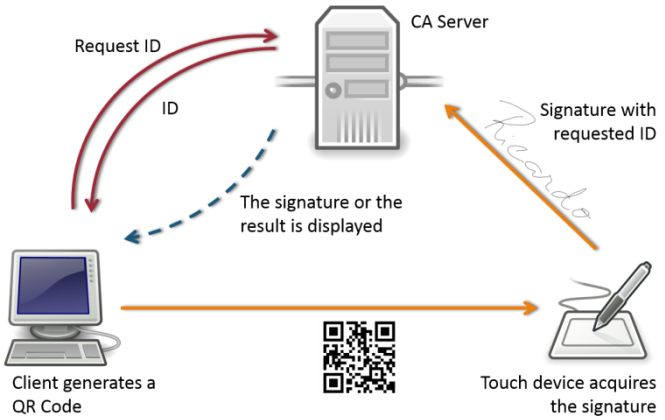

Figure 1. Architecture overview of the system

III. METHODS OF VERIFICATION

Handwritten signatures are very convenient and culturally very well accepted by the general population at large. Much less is known, however, about whether people perceive handwritten digital signatures on devices screens to be symbolically equivalent to traditional hand signatures on paper. Some studies demonstrate that although the functionally is the same, handwritten signatures on devices evoked markedly different psychological reactions than more traditional signatures written on paper. Namely, electronically handwritten signatures evoked a weaker sense of the signer's presence and involvement. This weaker sense of social presence, in turn, induced negativity: people were more likely to discount the validity of an e-signed application than of an identical application signed by hand directly on paper [1].

On other side, on the market, there is no an effective way to use handwritten signatures in digital documents in a secure way.

Signature verification may not be an easy problem to solve. We have to guarantee the authenticity of the user, but completely guarantee it is nearly impossible.

Since this system is a biometric system, FRR (False Rejection Rate) and FAR (False Acceptance Rate) rates are applied. As far as we are capable to reduce these rates, the better the biometric system becomes. The lower its EER (Equal Error Rate) the better is the biometric system.

A. *Types of verification*

There are two ways of using digital representations of handwritten signatures:

- **Offline or static** - in offline verification, the signature is drawn on paper and then digitized. The result is a bitmap image that can be incorporated as an image into any digital document that supports the inclusion of images. Since the image is simply scanned, all information regarding the time/space dynamics associated with the drawing of the signature are lost.
- **Online or dynamic** - in online verification, the signature is drawn on the digitizer device. There are specialized devices for this purpose, but general purpose devices like smartphones and tablets are also

able to acquire the signature. Specialized devices are better for acquire signatures because they have better resolutions and the result has more precision and feature dimensions. For example off the shelf tablets or smartphones do not have pressure sensors on their screens.

Our focus is on online authentication because it offers a much higher security level than offline signature verification [2].

B. *Verification Process*

The verification process is divided in several phases: data acquisition and preprocessing, feature extraction and classification [4]. Next is a brief explanation of each one:

- **Data acquisition and preprocessing** - first of all, the data should be acquired from the user by using a device. Then, the data should be preprocessed in order then to be stored.
- **Feature extraction** - in this phase, all features used on comparison are extracted from the signature, for example, if the method is based in acceleration, then acceleration should be extracted.
- **Classification** - after the features are extracted now is possible to compare the signatures and produce a result, saying if the signatures match or not.

C. *Data Acquisition*

The first step in handwritten signature verification is to acquire the signature. In the market there are several devices capable of acquiring digital representations of handwritten signatures. They can differ from each other allowing acquiring different parameters, thus changing the accuracy of the signature verification.

Mobile devices have been sold all around the world and they can also be effectively used to acquire the signature. Typically, they are able to acquire position, time, when the pen touch starts and when it ends. But there are specialized devices which are capable to acquire other parameters, like pressure, force, direction of movement and pen inclination [4].

Despite its apparent lack of sensory features when compared to more specialized devices, mobile phones constitute a good option because they are nowadays almost ubiquitous. However they can have a small input area and poor sampling frequency, making the signature data collection less accurate [3]. However we contend that just sampling pen position/time can be sufficient to accurately authenticate a user when he writes his signature on a smartphone or tablet screen.

D. *Verification Methods*

To verify a handwritten signatures is not easy and can be a complex task. The main goal is to guarantee that a forger cannot replicate the signature. It can be very difficult to achieve because if the forger knows exactly how the original signature should look like, with sufficient time and practice he will be able to forge it. It is therefore our objective to make the forger's task as hard as possible. Towards this goal we can employ several different signature verification methods.

Next we will present some of them and a small description:

- **Euclidean distance** – this method is based on distances measurements. The distance between the test signature and the reference signature should not exceed some threshold [4] [6].
- **Dynamic Time Warping** – this method measures the difference between two temporal series. Those temporal series can have different speeds (consecutively different accelerations), but the similarities can be detected in walking patterns. This algorithm was originally used in speech recognition [7].
- **Support vector machine** – this method is a type of learning machine for pattern recognition and regression problems, which constructs its solution in terms of a subset of the training data, the Support Vector. The method is popular in various pattern recognition problems because it provides very good results [8].
- **Neural networks** – this method is a statistical method used in machine learning and is inspired by biological neural networks (which is the case of brain) and are used to estimate or approximate functions with large inputs and those functions are generally unknown. Neural networks usually are systems of interconnected "neurons" which can compute values from the input [4] [9] [10]. An example of its use in handwriting recognition is neurons being activated by the pixels of an input image. Then the network is weighted and transformed by a function and the activations are passed to other neurons. This process is repeated until the output neuron is activated. Examples of neural networks are Bayesian, time-delay and back propagation networks [4] [9] [10].

IV. DISCUSSION

Our proposed verification method has been tested by sixteen people, each one of them drawing and checking his signature on the developed system. There were four people trying to forge those signatures, by just looking at them.

The algorithm used in this work to verify the signatures was the Euclidean distance, as mentioned before. This is a very simple and intuitive method that is also very easy to understand and to implement. It constitutes also a good way to start working and to become more knowledgeable about this subject. Our algorithm work as follows:

- First of all, the user has to register his signature. To do that, the system asks the user to sign five times. This is used by the system as training.
- Once these signatures are gathered, they are translated to the origin and scaled to the size of the biggest signature.
- The system then calculates the mean signature. The signature is segmented by touches and lift ups. Each segment will start when a touch down event is detected and will end when a touch up event occurs.

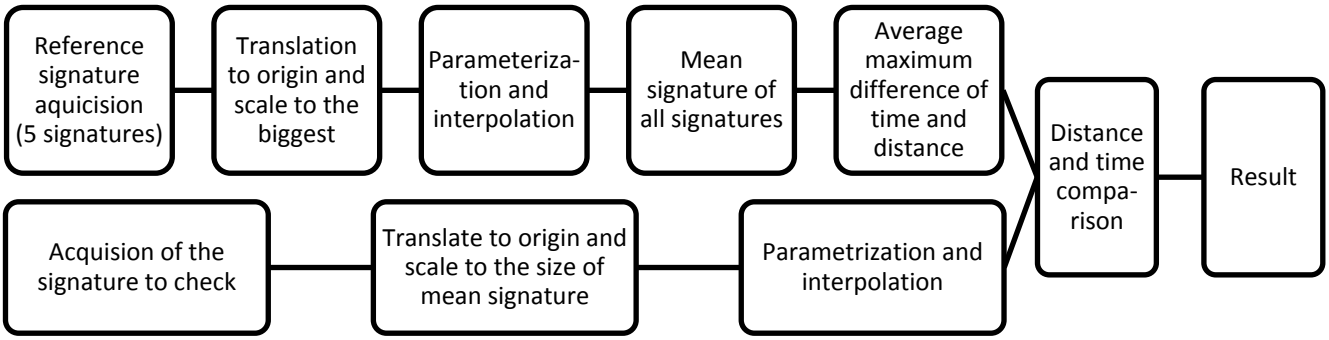

Figure 2. Verification process

- Each segment is parameterized and interpolated. The mean signature is calculated by doing the mean of all acquired signatures. This signature will be used as reference for future comparisons.
- We also calculate the average maximum distance and the average maximum difference time between all signatures.
- To verify if a signature matches with the reference signature, a similar process is used: it is also segmented, parameterized and interpolated in the same way. Then is compared the time difference and the distance between the signature and the mean signature. The distance should not exceed the values calculated in the previous step. If it exceeds, the algorithm will consider that the signature doesn't match.

On Fig. 2 we can see a diagram to better understand how all this process works.

The Fig. 3 shows what the input made by the user looks like and the resulting signature after calculating the mean signature.

(a)

(b)

Figure 3. Mean signature calculation. We can see a small dots indicating the sampling points. (a) The five signatures gathered from the user. (b) Result of mean signature calculation.

One big restriction of this method is requiring all signatures to have the same number of segments. This is intrinsically related with how the algorithm works. But, on practice, this cannot be a problem. Since each user will sign in the same way, he will produce a signature that will have always the same number of segments.

But sometimes this may not happen, especially if it is a forger. In this case, the algorithm answer immediately that the signatures does not match. This can happen because sometimes users can sign slightly different from time to time, or by imprecisions of the devices, or they can have some mistake during the drawing and they try to correct or simply by some intentional touch.

An important factor that might have implications in the results is the number of samples per second that the devices are able to read. If the number of points read is too low, this can lead to serious implications in the result, making it very inaccurate. With the tested devices, we were able get around 60 points per second, which is enough to have a good shape of the signature.

Other important parameters for signature recognition are, beyond read the position and the time, the pressure and the pen inclination. Using these parameters will increase the accuracy of the recognition because each user has its own characteristic way to apply force and incline the stylus against the touch device when writing. But, usual touch devices like smartphones are not able to detect these parameters, so we can't use them.

A. Results

First, we started by implementing the mean signature (parameterization and interpolation also because is required to calculate the mean) and the average maximum distance. Only with that, we were able to start to compare the signatures and get some results.

After, we implemented the translation to origin and signature scaling. The translation to origin will allow to the place where the user signs not influence the results. If the translation is not applied, the user can sign a bit far from where usually signs and the algorithm will produce a negative answer. Regarding to scaling, this allows to the process to be independent of the size which with the user signs. The main reason is because we want the device's size do not influence. If the signature is made in a bigger device, the users tend to draw bigger and vice versa.

But by using this method make it even hard for signature's author to verify his own signature, especially if the calculated values for average distance and time are small. On the one hand, we want make it easy for authors verify his signature, but on the other hand, we want it hard verify positively a forged signature. This point is known as EER (Equal Error Rate), is when FRR (False Rejection Rate) equals FAR (False Acceptance Rate).

In order to improve the method, we started multiplying the average maximum distance by a multiplier, increasing (or decreasing if smaller than one) the space where the signature can land in comparison with reference signature.

By analyzing TABLE I. we can determine what the best multiplier for the average maximum distance is. The table is sorted by the column EER and the value shown is the difference between FRR and FAR. The column Distance Mult is intended as the multiplier, and Author Accept, Author Reject, Forger Accept and Forger Reject the number of signatures with the respective description.

TABLE I. AVERAGE MAXIMUM DISTANCE MULTIPLER

Distance Mult	Author Accept	Author Reject	Forger Accept	Forger Reject	FRR	FAR	EER
0,0	0	28	0	41	1	0	1
0,7	1	27	0	41	0,9643	0	0,96429
1,0	5	23	1	40	0,8214	0,0244	0,79704
1,5	18	10	8	33	0,3571	0,1951	0,16202
1,6	18	10	12	29	0,3571	0,2927	0,06446
1,7	19	9	13	28	0,3214	0,3171	0,00436
1,8	22	6	15	26	0,2143	0,3659	-0,1516
1,9	23	5	15	26	0,1786	0,3659	-0,1873
2,0	23	5	16	25	0,1786	0,3902	-0,2117
2,5	25	3	22	19	0,1071	0,5366	-0,4294
3,0	27	1	23	18	0,0357	0,561	-0,5253

So, we conclude the best multiplier is 1.7, which have the EER value closer to 0.

But, until now, we have just dealt with distances comparisons. We can still improve the results by including the time in the process. Next, we will talk about the implementation of these improvements and results it achieves. To implement time verification, we can apply a similar method that we have done for distance.

When calculating the mean signature, the mean time can be also calculated. Each segment can be parameterized and interpolated in time, like what has been previously done for time. When the average maximum distance is being calculated, we can also calculate the average maximum difference time in the same way.

Like what happened before for distance, if the average value for time is used, it makes harder to verify positively the signature. So, we have to introduce a multiplier for the average time, making the time window larger.

On TABLE II. we can see the study of the multipliers variation. But now, there are two parameters that can change: the multiplier for time and for distance. The table is sorted by EER (which is the difference between FRR and FAR) and it could be extensively long, so some values are missing.

TABLE II. AVERAGE TIME DIFFERENCE AND DISTANCE MULTIPLIERS

Time Mult	Distance Mult	Author Accept	Author Reject	Forger Accept	Forger Reject	FRR	FAR	EER
0,5	0,5	0	28	0	41	1	0	1
1,0	1,0	1	27	0	41	0,9643	0	0,96429
2,0	1,0	4	24	0	41	0,8571	0	0,85714
1,0	2,0	7	21	0	41	0,7500	0	0,75000
1,5	4,0	12	16	3	38	0,5714	0,0732	0,49826
2,0	2,0	14	14	1	40	0,5000	0,0244	0,47561
4,5	1,5	17	11	4	37	0,3929	0,0976	0,2953
2,5	3,5	17	11	5	36	0,3929	0,1220	0,27091
3,5	2,5	20	8	9	32	0,2857	0,2195	0,0662
3,0	4,0	18	10	12	29	0,3571	0,2927	0,06446
4,0	2,5	21	7	9	32	0,2500	0,2195	0,03049
3,4	3,3	20	8	11	30	0,2857	0,2683	0,01742
3,4	3,4	20	8	11	30	0,2857	0,2683	0,01742
3,5	2,9	21	7	10	31	0,2500	0,2439	0,0061
3,6	2,9	21	7	10	31	0,2500	0,2439	0,0061
3,6	3,0	21	7	10	31	0,2500	0,2439	0,0061
3,6	3,1	21	7	10	31	0,2500	0,2439	0,0061
3,7	2,6	22	6	9	32	0,2143	0,2195	-0,0052
3,7	2,7	22	6	9	32	0,2143	0,2195	-0,0052
3,7	2,8	22	6	9	32	0,2143	0,2195	-0,0052
3,8	2,6	22	6	9	32	0,2143	0,2195	-0,0052
3,8	2,7	22	6	9	32	0,2143	0,2195	-0,0052
3,8	2,8	22	6	9	32	0,2143	0,2195	-0,0052
3,9	2,6	22	6	9	32	0,2143	0,2195	-0,0052
3,9	2,7	22	6	9	32	0,2143	0,2195	-0,0052
3,9	2,8	22	6	9	32	0,2143	0,2195	-0,0052
3,2	3,7	20	8	12	29	0,2857	0,2927	-0,0070
4,0	3,0	22	6	10	31	0,2143	0,2439	-0,0296
4,5	2,5	23	5	9	32	0,1786	0,2195	-0,0409
3,5	3,5	21	7	12	29	0,2500	0,2927	-0,0427
4,0	3,5	22	6	12	29	0,2143	0,2927	-0,0784
4,5	3,0	24	4	10	31	0,1429	0,2439	-0,1011
4,0	4,0	22	6	13	28	0,2143	0,3171	-0,1028
4,5	3,5	24	4	12	29	0,1429	0,2927	-0,1498

Looking at the table, the best values are 3.7 for time multiplier and 2.6 for distance multiplier, but there some entries with the same value for EER. Once the EER value is negative, the best answer will be upwards, meaning in this case the smaller multipliers.

Using the time in the signature verification, we were able to make it around 10% more effective, not only by giving better results for false positives, but also by improving the false negatives.

V. CONCLUSION

Using the Euclidean Distance it is possible to start verifying handwritten signatures by just using distances. It is also possible to obtain meaningful authentication results that tell us whether it is the legitimate user which is signing or if he is being impersonated by some other person.

However if a user is specialized in forging signatures, he will probably be able to make a successful forgery. If the legitimate user creates his reference signature based on more similar signatures, it will help to avoid this problem because the means for time and distance will be smaller.

Using the time dimension for the verification process improves the results. In this case, the improvement was 10%.

We believe that further refining the all process by using speed and acceleration will help to achieve better results.

Handwritten signature verification is an important step for the general massification of digital legal documents. The main reason being the use of handwritten signatures in documents still is, and will be in the foreseeable future, the culturally dominating accepted form of authenticating them.

VI. Future Work

The method proposed in this work is still far from being able to be considered safe to be used on real applications. Nowadays does not yet exists a well-accepted solution to this problem and this constitutes an active area of research where it is still possible to make very meaningful contributions.

In order to achieve better results, we will have to implement a more efficient method. A good option could be Bayesian Neural Networks because it enables to learn the very characteristics of the signer and making the recognition more accurate.

The testing process also has to be improved. The number of signers and forgers should be larger in order to test a variety of situations, closer as possible to reality. To do so it is planned to publish the system with CRACS/INESC members, which are around 750 members.

Another improvement to be made is to test the system with devices that are able to acquire pressure and inclination to compare with the accuracy achieved by simply using time/positioning and thus better understand how these extra parameters could affect the result and what the real practical improvements that could be obtained with a larger dimension space set of biometric features.

Acknowledgements

This work is financed by the FCT – Fundação para a Ciência e a Tecnologia (Portuguese Foundation for Science and Technology) within project UID/EEA/50014/2013.

References

[1] E. Y. Chou. “Paperless and Soulless: E-signatures Diminish the Signer’s Presence and Decrease Acceptance,” Social Psychological and Personality Science, pp. 1-9 , December 2014.

[2] C. Gruber, C. Hook, and J. Kempf, G. Scharfenberg and B. Sick. “A Flexible Architecture for Online Signature Verification Based on a Novel Biometric Pen,” 2006 IEEE Mountain Workshop on Adaptive and Learning Systems, pp. 110-115, July 2006.

[3] D. Impedovo, G. Pirlo, and R. Plamondon, “Handwritten Signature Verification: New Advancements and Open Issues,” 2012 International Conference on Frontiers in Handwriting Recognition, pp. 367-372, September 2012.

[4] D. Impedovo, and G. Pirlo. “Automatic Signature Verification: The State of the Art,” IEEE Transactions on Systems, Man, and Cybernetics, vol. 38, no. 5, pp. 609-635, September 2008

[5] R. S. A. Araujo, G. D. C. Cavalcanti, and E. C. D. B. C. Filho, “On-line verification for signatures of different sizes,” 10th International Workshop Frontiers in Handwriting Recognition, La Baule, France, October 2006

[6] M. K. Khan, M. A. Khan, M. A. U. Khan, and I. Ahmad, “On-line signature verification by exploiting inter-feature dependencies,” 18th International Conference on Pattern Recognition, pp. 796–799, August 2016

[7] R. Martens and L. Claesen, “On-line signature verification by dynamic time-warping,” 13th International Conference on Pattern Recognition (ICPR96), Vienna, Austria, 1996, pp. 38–42

[8] S. Fauziyah, O. Azlina, B. Mardiana, A. M. Zahariah, and H. Haroon, “Signature verification system using Support Vector Machine,” 6th International Symposium on Mechatronics and its Applications, vol., no., pp.1,4, 23-26, March 2009

[9] M. Khalid, H. Mokayed, R. Yusof, and O. Ono, “Online Signature Verification with Neural Networks Classifier and Fuzzy Inference,” Asia International Conference on Modelling & Simulation, pp. 236-241, 2009

[10] A. McCabe, J. Trevathan, and W. Read, “Neural Network-based Handwritten Signature Verification,” Journal of Computers, vol. 3, no. 8, August 2008