

OFFLINE HAND WRITTEN SIGNATURE VERIFICATION BY USING GREY-SCALE DATA BASE DISTORTION

T Vijay¹, V Nagi Reddy²

¹M.Tech (CS) Scholar, ²Assistant Professor

Nalanda Institute of Engg and Tech. (NIET), Siddharth Nagar, Guntur, A.P, (India)

ABSTRACT

Signature of human is an important utility for all the transaction; it was involved like a main door for many things in human life to access the authentication identity in real time. We can take biometric system and voice reorganization etc are the examples for the personal identification in present situation. In the same way human hand made signature also considered to for the personal identification in natural way. Off-line signature verification is fully based on local system verification method, it works locally to encode and to translate the image into binary format. When the signature was uploaded it will compare with the existing signatures from the database and it will contain more related signatures for the future verification process. For that reason herewe are introduced MCYT database signature verification system for the local system. In the time of verification it will extract the informational and translate it into geometric network fro the checking purpose. After the verification user can perform the transaction.

Keywords: *Security, Authentication, Online Signature Verification, Offline Signature Verification and Network*

I. INTRODUCTION

To check the authentication process we need to verify their authentication validation. For that we have implemented some of the applications with the help of robust deification method for the identification of humans' exclusively crosswise in the world. Like an example we have biometric finger printing and handmade signatures and face scanning etc. In the midst of these entire handmade signatures plays an important role in some of the business applications, through this signature many transactions are happening for both the private and public sectors. This signature verification technology is mainly involved on different monetary transactions. We can check this process in entire the world. System signature verification is different when we compare to human hand made signature. Because it will depend upon the person and time of his psychology and its complex process when we check it with the existing system process, for this we were used twotypes of methodologies to check the signature one is offline signature verification. We use optimal scanner for the offline verification and it we go for the other one it's online one it will be more efficient than the signature scanning. It has to perform the actions like to check the human psychology to guess the signature. For that we have to get the dynamic information about the approach to control the process in application. Here is three kinds of approaches was mentioned that is methods and method implemented analyse operations. For this two kinds of performances data accessing was used that means for the higher pressure points and lower demandsin network.

If we take a general example person signature will change automatically, not at all the times but it may not be the same every time based on the document and it will identify the documented based signature of its related work it will be depend upon its assumption. Similarly we have some of the identification factors in real time sector it's like the face scanning and biometric signature verification etc. When we observe the image or face detection it has to scan and check the each coordinates of the files information in the sector. And it's May not easy to identify and scan the face for that we have to identify the total image sometimes. If we take the signature for that no need of take and observe the total image which was assigned to check. Signature contains only the characters and the letters and it's the combination of the factors and its related its factors. First thing is to make sure that we are checking only the signature which was made by the human. It's the process of checking and identification of images from the database which was related to the users. For the verification process it will use the binary code fit ratio in the application it will be used between 0's and 1's only. For the identification we have two types of attribute verification methods that is write the signature or text directly on the puerperal devices and another thing is to upload the image and to scan that image with the comparison of existing one.

OCR (optical Character Reorganization) is the main stream for the technical identification. For the security reasons in shopping websites users are used this signature verification to identify the valid suer and to identify the user hand writing signature and it will translate that into text format for the substantiation in network. Based on this we can simply translate and resolve the process of identification by send it to binary code information and it can simply translate that into binary code format.

1.1 Offline Signature Verification

We are introduced two kinds of databases for offline signature verification. They are MCYT Database and Gray Signature Database. For the MCYT have the 15 signatures as a genuine And it will be store in database with the combination of its related signatures and appropriated images to the signature it will store in database. So based on stored signatures in database we will verify the signature or invoice it. In gray signature data base we have more than 200 genuine signatures it will provide its related to the combination of different types of identification colour based and attribute based related information towards the signature in database for the identification. To observe the curve aspect of the signature, and it will convert all the samples of signature into black and white background and it will eliminate the remaining thing in the time of scanning. We can check that on bellow sample signature image.

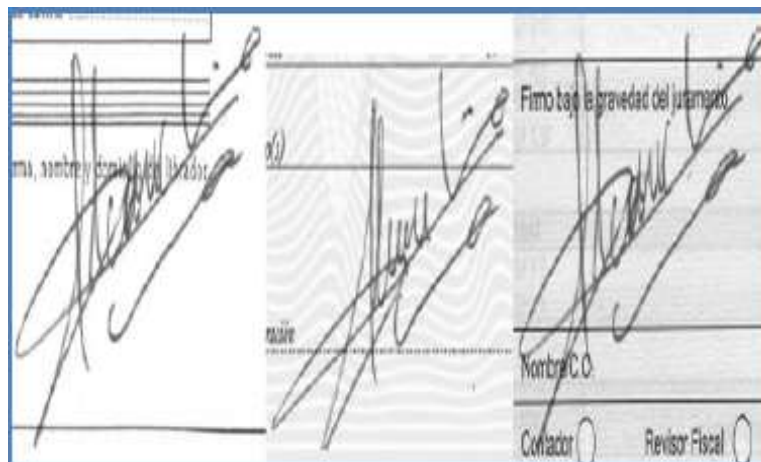


Fig1 signature with the Varied Background

For the implementation of posturised images we are implemented this two types of data bases for the processing we have to follow this:

$$I_p(x, y) = \text{round} \left(\text{round} \left(\frac{I(x, y) \cdot n_i}{255} \right) \cdot \frac{255}{n_i} \right)$$

For the signature verification it process it for the segment to carried out till the conversion of image from original so black and white or the gray colour related image and with its characteristics we can see in the bellow example:

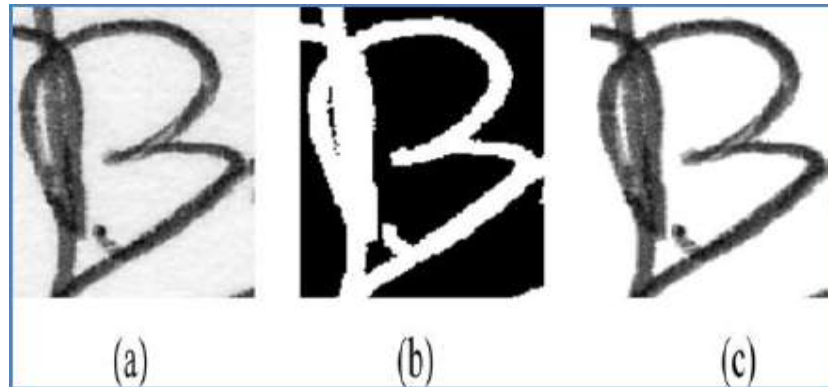


Fig2: Segmentation of Image

Here it will show clearly about the offline signature verification of user handmade signature and it will translate image into black and white and it will reduce its size and zoom optics of image identification in the time of scanning.

II. RELATED WORK

Here in this paper we introduced an advanced property of identification performance of image for the highly acceptance. After the signature acceptance and to identify the authentication of users and making the validation if the assigned signature is valid then it will proceed for the acceptance of transaction, or else it will stop the accessing permission. For this verification we are using more than 40 methodologies and as well as this process has differed into two categories that is local and global. In the local session it will check or select the particular point or the dimension of the image which was mentioned and global session is for the total session to identify and to maintain that all the information as well as to check the total image containing of the signature and its related textual box of image content everything it will check.

Mostly the online signature system preserves the sensitive data of the image and for that we have involved genetic algorithm for the best feature in online signature verification. So everything of information will be maintained as a sample pack in the system. It makes to involve in the system and to obtain the information of the images and to delete the old information and then after that it will do the comparison and the validation process for the image verification or scanning. When it was compared with the other image it will be consider all the partitions and each and everything of characters list which was assigned in to binary code, it will verify that binary information.

For the online signature verification recovery we have to need some of the peripheral devices and we need to count the speed of the hand and as well as the time interval to measure the human hand speed in the time of human signature writing on puerperal devices. If we came to check the offline signature verification it will consider the process of biometric as implementation signature verification for the system. Biometric process the

verification of person identity of human and it will be based on physical attributes of human. In biometric system also there were a lot of security tasks, that is fingerprint and heart sound identification like this more of the applications was implemented for the security reasons in the biometric system.

After the image uploading for the verification it will check the process under the power consumption and the use case of system. And it will be based on attributes to make in well stable situations based on the layers which were applied to the relabel to the outcome of the process. The generated part of the image will represent its functionality related to the attributes for the functions. After that it will make a tool for the coping of image with the different layouts and it will inherit that all things related to its directions for the handmade signature. Then it will protect the sensitive data of image and it will take the best in it after the network topology for the image noise mode and to check the performance of it. Then after it will perform the degradation of the processing based on the conditions. Finally it will execute this process for the identification of factors to arrange the data based on the large amount or lowest amount. It will count the time interval of the process and it will check the process of time intervals when human is making the sign on puerperal devices. In this paper we proposed HSV based and NN based architecture for the signature verification in different conditions. After the performance of all the division parts it will check the condition of image updating status and then it will declare the result of image.

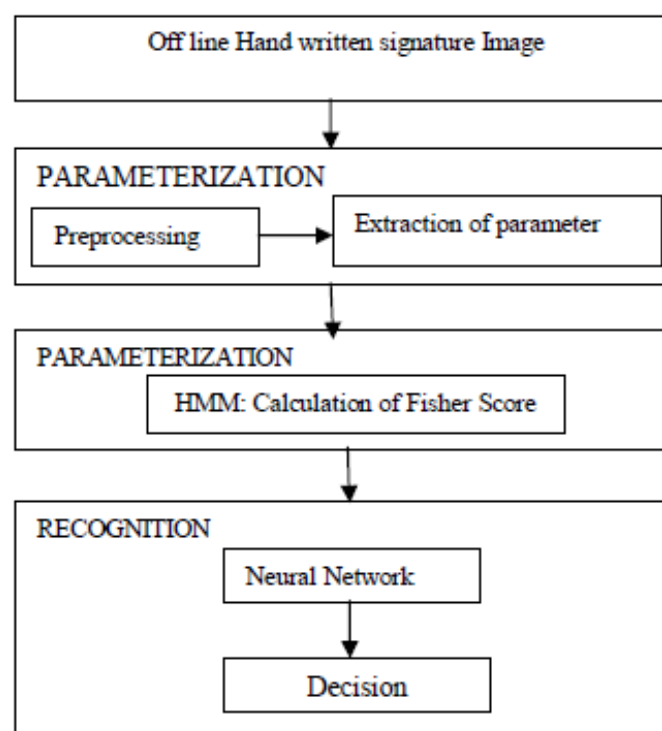


Fig3: Signature Verification Process

By the following of these steps we can proceed for the identification factor and for the signature verification. It will check finally the authentication process to release the user if the signature is valid of an authenticated person it will release human to access the account transaction as usual in that network. When the process was in training stage it will just pass all the steps to check the signature in online and offline mode. After the completion of the training stage it has to retrieve the images from the data base to compare the human made signature. After the completion of retrieving it will split that image in to the layers and transfer it into binary format to communicate easily.

III. RESULTS

The proposed system was implemented on vector based cases to retrieve the information and to check the data. Here the horizontal lanes will describe about probability density of vertex axis function. Then it will show the form of output and divide that based on the performance of the graph like low level medium and high level performance of the signature verification and the distribution process of retrieving the image from Gray Scale database and to compare with the existence of the images based on its vertices. We can observe the gray scale result in below graph which was representing the process of signature verification in gray scale data base retrieving.

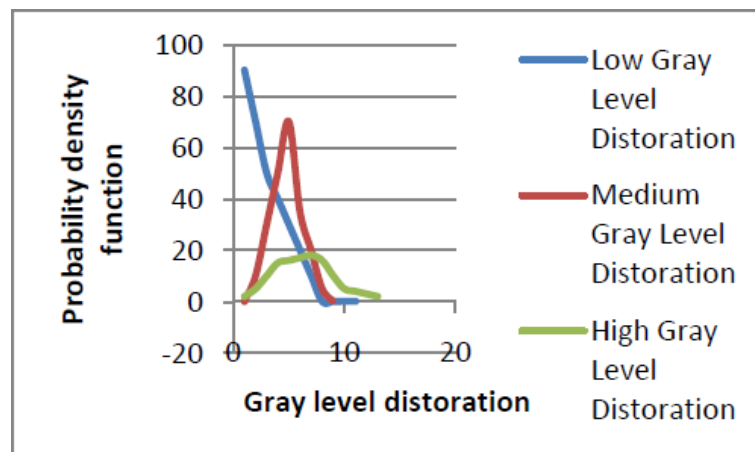


Fig4: Gray Level Data Base Distortion

When we compare and check the gray scale it will give the results as above diagram, in the same way after the comparison there may be some of the situations it may fail the condition authentication. Thenafter it we will collect that information in another database and we are drawn in another graph that all the conditions we can check here for the identification of conditions failed situations in the graph.

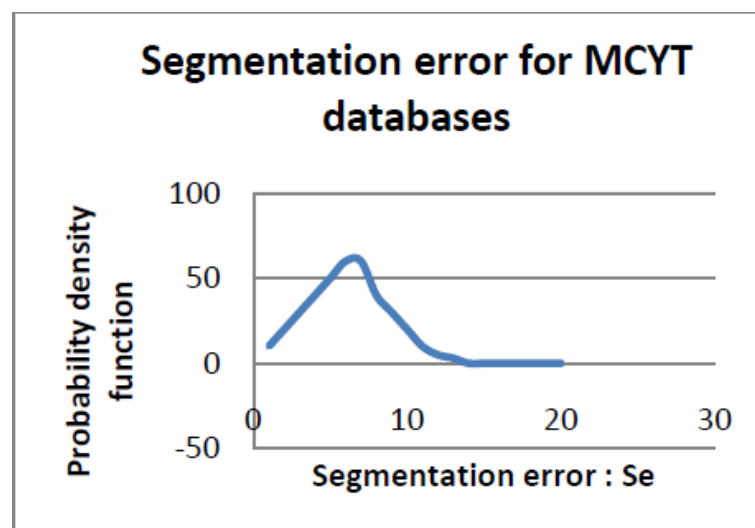


Fig5: Segmentation Error Identification

When the condition of verification pass to true 100% then only it will allow the user to access and to authenticate the things from the data base, then that human be authenticated person he could access the transaction of paging on the application.



IV. CONCLUSION

Here we are introduced online signature verification for the human authentication in the network. There were different patterns to verify the signature that is local and global binary transmission methods to evaluate the classified user's information and to verify the output. For the verification we are used Histogram oriented and the kernel based functionality was implemented SVM. Basic concept is to verify the offline signature which was written by the human. We were implemented this as a proof for the demonstrating of application. We can do this both ways of invoice and checking of signature automatically when we write the signature on puerperal devices. After uploading of signature it will compare with the existing proofs and make final with the gray scale mode. At final user can be allowed to get the permission to make the transaction after he signature verification was passed.

V. REFERENCES

- [1] D. Impedovo and G. Pirlo, —Automatic signature verification: The state of the art,|| *IEEE Trans. Syst. Man Cybern.—Part C: Applications Rev.*, vol. 38, no. 5, pp. 609–635, Sep. 2008.
- [2] W. Hou, X. Ye, and K. Wang, —A survey of off-line signature verification,|| in *Proc. Int. Conf. Intelligent Mechatronics Automation*, Chengdu, China, Aug. 2004, pp. 536–541.
- [3] J. Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez, and J. Ortega-Garcia, —An off-line signature verification system based on fusion of local and global information,|| in *Proc. Workshop Biometric Authentication*, Springer LNCS-3087, May 2004, pp. 298–306.
- [4] M. Ammar, Y. Yoshida, and T. Fukumura, —A new effective approach for automatic off-line verification of signatures by using pressure features,|| in *Proc. 8th Int. Conf. Pattern Recognition*, 1986, pp. 566–569.
- [5] A. Mitra, P. Kumar, and C. Ardil, —Automatic authentication of hand-written documents via low density pixel measurements,|| *Int. J. Computational Intell.*, vol. 2, no. 44, pp. 219–223, 2005.
- [6] H. Lv, W. Wang, C. Wang, and Q. Zhuo, —Off-line Chinese signature verification based on support vector machine,|| *Pattern Recognition Lett.*, vol. 26, pp. 2390–2399, 2005.
- [7] J. Vargas, M. Ferrer, C. Travieso, and J. Alonso, —Off-line signature verification based on high pressure polar distribution,|| in *Proc. Int. Conf. Frontiers of Handwriting Recognition 2008*, Montreal, Canada, 2008

AUTHOR PROFILE

	<p>T Vijay is currently pursuing M.Tech in the Department of Computer Science, from Nalanda Institute of Engineering & Technology (NIET), Siddharth Nagar, Kantepudi (V), Sattenapalli (M), Guntur (D), Andhra Pradesh, Affiliated to JNTU-KAKINADA.</p>
	<p>V Nagi Reddy working as Assistant Professor at Nalanda Institute of Engineering & Technology (NIET), Siddharth Nagar, Kantepudi (V), Sattenapalli (M), Guntur (D), Andhra Pradesh, Affiliated to JNTU-KAKINADA.</p>