IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SIGNATURE VERIFICATION

[1]J.Mary Angeline,[2]A.Anitta,[3]S.Devi Bala,[4]K.Muthu Selvi,[5]A.Yogeswari,

[1]Faculty,[2,3,4,5]UG scholar,
Computer Science and Engineering,
[1]JayarajAnnapackiam CSI College of Engineering, Nazareth, India

Abstract: Technology Security is a crucial component of the field of information to prevent forgery and guarantee data security. Authentication is crucial component of security management. A person's signature serves as a physical representation of who he is. A customer's signature on a document represents an instruction from him to the Bank to carry out an authorized transaction on his behalf. In the area of information technology security, preventing forgery and ensuring information confidentiality are integral parts of it. Authentication is a crucial component of security management. In essence, this project involves applying a certain type of machine learning algorithm on photographs of customer signature that banks have.

***Index Terms* – verifying face and signature.**

I. INTRODUCTION

A person's signature serves as a physical representation of who he is. A customer's signature on a document is an instruction to the Bank to carry out an authorized transaction on his behalf. In the area of information technology security, preventing forgery and ensuring information confidentiality are integral parts of it. Authentication is crucial in the fight against security threats. This is essentially a form of machine learning algorithm that you would apply to photos of customer signature that banks hold, and the algorithm would compare these to forgeries to determine whether the signature provided while making a cheque payment or DD payment is true or not. This project's goal is to make sure that the delivered services.

II. LITERATUREREVIEW

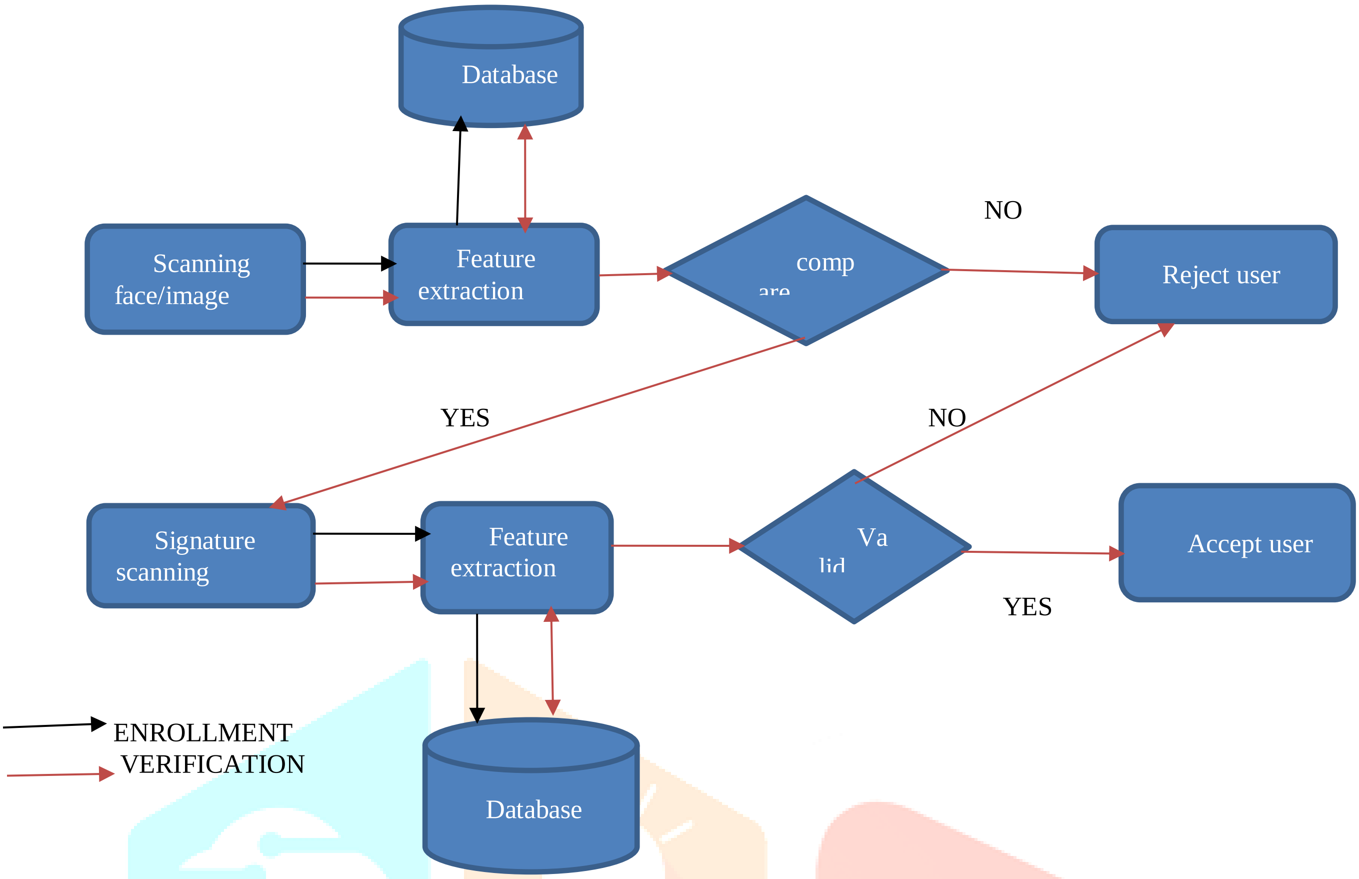
Harika et.al. have utilized the 2 publically available databases for the experiment. The first one is known as MCYT database, which has signature from 75 genuine signs. For each signer 15 forged signature and 15 genuine signature are taken and stored in the database. The second database is known as the GPDS60. Gray signature which has signatures collected from 881 signs. The databases contains signatures in the form of checks or invoices. The blending modes that are used during experimentation include linear born , color, lighten, multiply and darken. For processing of signature only signature strokes are considered, the signature samples has white background.

Darmola et.al. have presented an offline signature recognition system by using Hidden Markov Model and discrete cosine transform. The signature were divided vertically into the segments at center of gravity, this division was carried out with the help of pixels reference positions. The results of this experimentation showed that 99.2% correct signature recognition rate is possible.

Abbas et.al. have proposed a system for managing SVM classifier conflicts. This system based on the decision combination rule that base on generalization belief function of desert Snarabdache theory The SVM outputs are merged by this framework and use the technique of estimation.

Pansare et.al. presents a method which consists of image processing, geometric features extraction, neural network training with extract features and verification. Verification stage includes applying the extracted features of test signature to a trained neural network which was used to classify it as a genuine or forged.

III. RESEARCH METHODOLOGY



3.1 USER REGISTRATION

You can design and develop the ideal user registration forms for your website with the aid of the user registration form module of ultimate Add for Beaver builder. Using this module, you may also choose to auto-login, send an email after a successful registration, or redirect the user to a custom URL.

3.2 USER LOGIN

When users reach the URL for blackboard learn through portal direct entry, the gateway and login pages are skipped. Users instead view the top-level portal tab. Users who enter the system through portal direct entry are treated as visitors until they log in. users can login by entering their user name and password in the portal module known as the login module. To enable users to log in to the system, you may add this module to any module tab.

3.3 FEATURE EXTRACTION

Using Siamese Convolution neural network model, features from the input signature and previously stored signature are extracted. Different signature specifications are used by signature verification systems. The accuracy of the signature verification method is highly dependent on the features that are chosen for extraction. Due to the many signature shapes and sampling circumstances, it is also the most challenging stage of the signature verification system. Any signature verification system's feature extraction procedure is a key challenge. Even the accuracy of two people's true signature cannot be guaranteed. The fact that expert forgeries replicate the real pattern adds to its complexity.

3.4 FACE RECOGNITION

A robot is used in the recognition process to detect faces utilizing the PCA, LDA, and LBPH algorithms, which are include into the open cv package. The face detection process will once more be carried out by the robot as it moves and captures the photographs in real time. The robot has four wheels and a 10pm rustler wheel. To allow the camera and its proper resolution to recognize faces, the speed should be slow.

3.5 COMPARISON

Using distance matrix, determine how far apart the input signature is from previously stored signatures. The lowest, average, and maximum values of the dissimilarity values are used to compare the test signature and reference signature after the feature extraction method has been applied. One can determine whether a signature is a fake or authentic one by selecting one of the dissimilarity values listed above. For both the reference and test signatures, a threshold value is used in this comparison. If the value is roughly identical to the reference signal value, the signature is accepted as authentic; otherwise, if the difference is greater than that threshold value, the signature is disregarded. This cutoff is possible.

3.6 VERIFICATION ENROLLMENT

The test signature and reference signature are compared using the minimum, average, and maximum values of dissimilarities after the feature extraction method has been applied. Picking any it is decided whether it is a fake based on the aforementioned value, of dissimilarity. Either a true signature or a signature. Using a threshold value, this comparison is made. For all of the test signatures and references. If the amount is roughly equal to then it is regarded to be a legitimate signature and if the reference signal value is greater than if the degree of dissimilarity exceeds that cutoff, the signature is not accepted. This either the threshold value is the same for every signature or it can be different regarding each of them.

IV. RESULTS AND DISCUSSION

We discussed various learning representations for offline signature verification formulations in this research. Convolution Neural Networks are superior for the classification of signatures, according to an analysis of the aforementioned data. By understanding the visual clues, anyone can develop the intuition to distinguish between real signatures and fakes with increased accuracy. The new design, which was motivated by Google Net and functioned more broadly then diving deeper, is also responsible for the huge gain in accuracy. Therefore, it is evident from the aforementioned experimental findings that the inception SVG Net Architecture is more effective at finding patterns in images by leveraging bigger networks. Future research will follow this pattern as academics continue to look for improved feature sets and methodologies.

4.1 SAMPLE SCREENSHOT

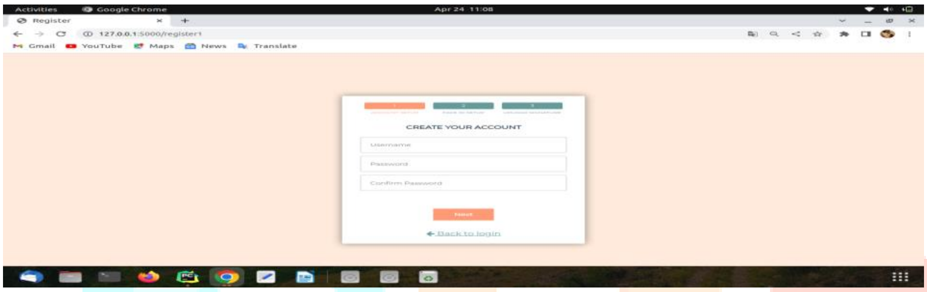
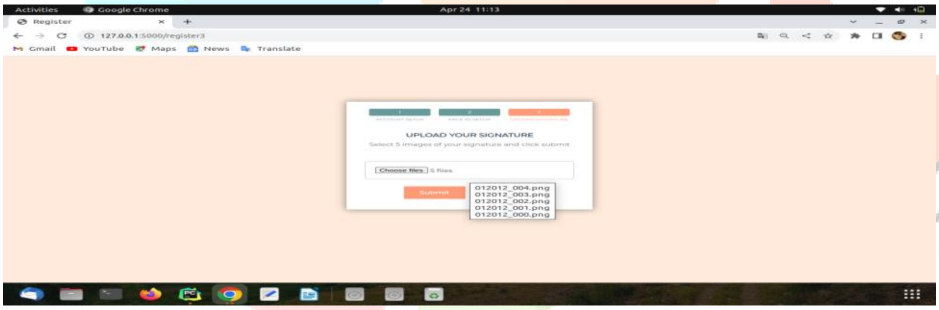


Fig 1 Register page

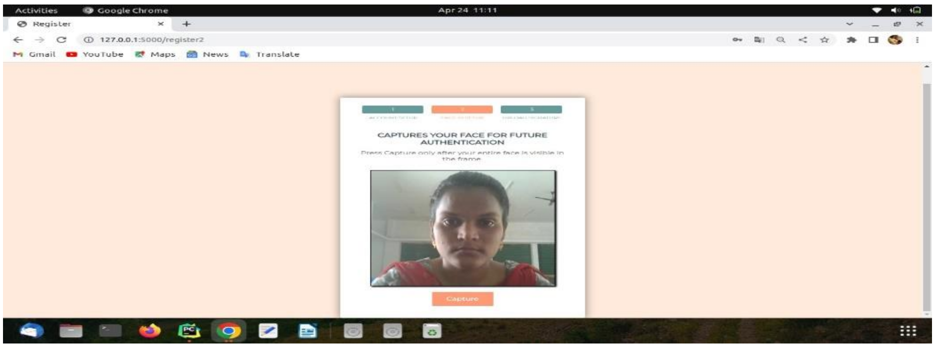


Select 5 images of your signature and click submit

5 files

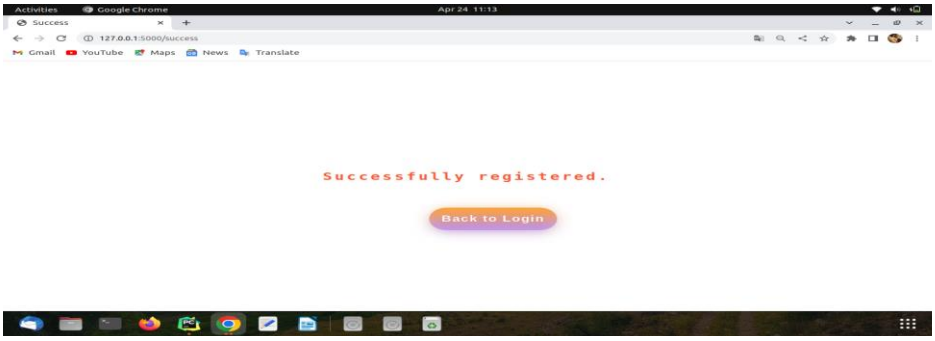
012012_004.png
012012_003.png
012012_002.png
012012_001.png
012012_000.png

Fig 2 Add signatures image



Press Capture only after your entire face is visible in the frame

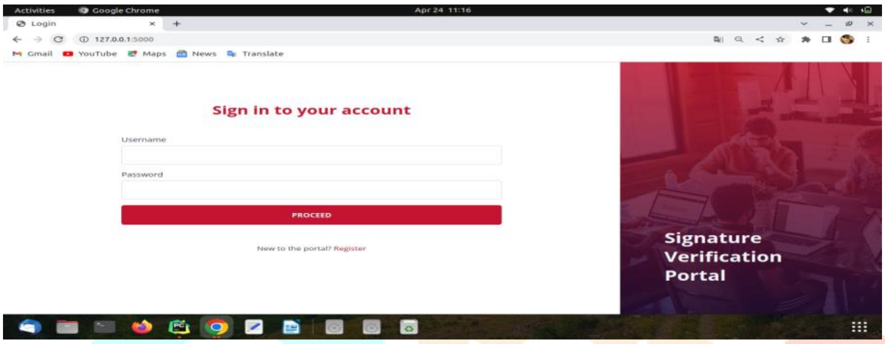
Fig 3 add face image



Successfully registered.

Back to Login

Fig 4 registered successfully



Sign in to your account

Username

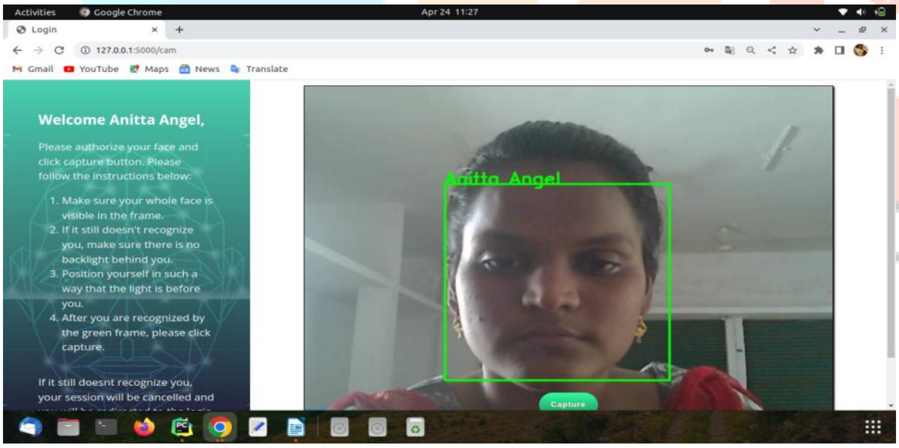
Password

PROCEED

New to the portal? Register

Signature Verification Portal

Fig 5 Login page



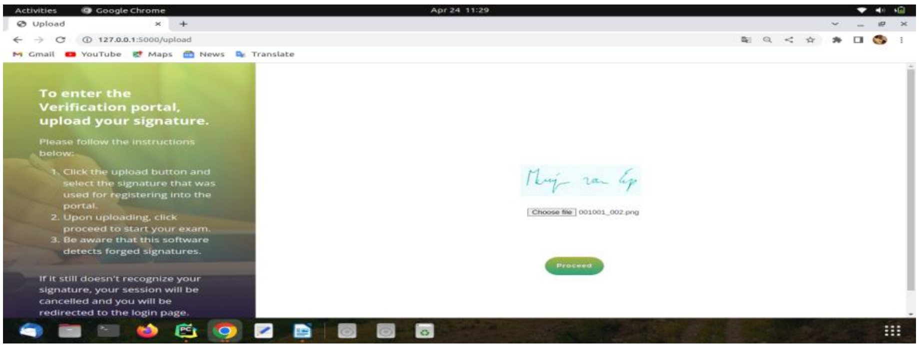
Welcome Anitta Angel,

Please authorize your face and click capture button. Please follow the instructions below:

1. Make sure your whole face is visible in the frame.
2. If it still doesn't recognize you, make sure there is no backlight behind you.
3. Position yourself in such a way that the light is before you.
4. After you are recognized by the green frame, please click capture.

If it still doesnt recognize you, your session will be cancelled and

Fig 6 Face scanning



To enter the Verification portal, upload your signature.

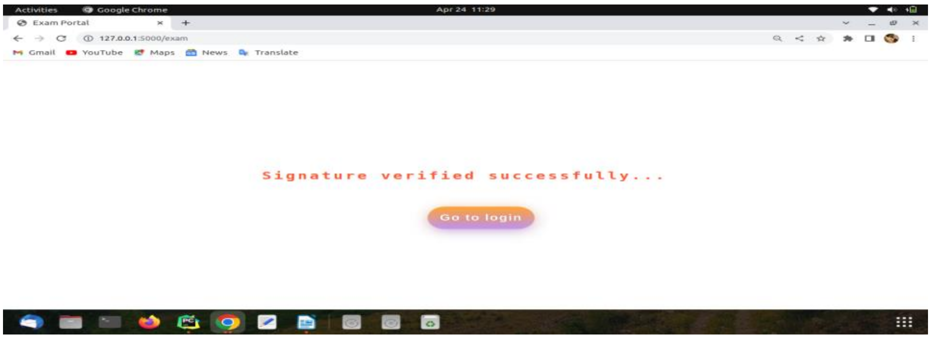
Please follow the instructions below:

1. Click the upload button and select the signature that was used for registering into the portal.
2. Upon uploading, click proceed to start your exam.
3. Be aware that this software detects forged signatures.

If it still doesn't recognize your signature, your session will be cancelled and you will be redirected to the login page.

001001_002.png

Fig 7 verifying signature



Signature verified successfully...

Fig 8 Signature verified

V. FUTURE ENHANCEMENT

As the database increases the computational time of offline signature verification system increases. And the dynamic information is lost using this method. Dynamic information is much more efficient than the static information which we have used in this. Hence as a future work we can design a system which is a combination of static and dynamic information i.e., the combination of offline and online verification systems. Or we can design an On-line signature verification system which is purely based on dynamic features which is much more efficient than this.

VI. ACKNOWLEDGMENT

We would like to acknowledge our sincere thanks to the management of our college and our family members who have supported and helped us in different stages of this project work.

REFERENCES

[1] K.Harika,& T.C.S. Ready, “ A tool for Robust offline signature verification ” , International Journal of advanced Research in computer & communication Engineering, volume-2,p.p 3420,sept.2013.

[2] D.S.A.Daramota, & p.t.sibiyemi, “ Offline Signature Recognition using hidden marks, model “ ,International journal of computer Application, volume-10,pp.17-22,November 2010.

[3] N.Abbas; and Chibani; “SVM-DSMT combination for off line signature verification,” International conference on computer information and tele-communication system .pp 45-56,May 2012.

[4] Pansare.Ahisini, Bhatia.Shalini, “How written signature verification using neural network” , International journal of applied information system, volume-1,.NO-2,pp-44-49 Jan 2012.