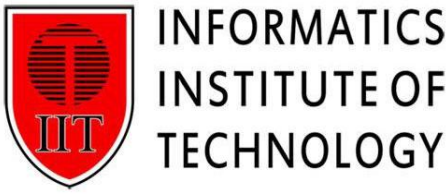

Informatics Institute of Technology

Department of Computing

Software Development Group Project

(5COSC009C)

Module Leader - Mr.Banuka Athuraliya

Literature Review Submission

Online Identity Verification & Authorization Platform

Team - ZipCode

Team Members	IIT ID	UoW ID
Apiseg Rajendran	2018086	w1761737
Gibran Kasif	2019176	w1761211
Alexio Peiris	2018110	w1761873
Disura Randunu	2018008	w1761865
Osanda Ginige	2018181	w1761754
Danuja Silva	2018221	w1761772

LITERATURE REVIEW

Introduction

As mentioned in the previous chapter online identity verification has been a major field of research for years now. All the previous researches can be categorized into the following topics.

1. Facial recognition and liveness detection
2. ID verification
3. Handwritten signature identification

Once the facial recognition systems were introduced, they were met with a problem where those systems were not able to authenticate if the user is physically there or a mere photograph of the user is being used. This issue had to be rectified in order to make the facial authentication process more reliable(Tan et al., 2010).

The handwritten signature holds a very important place in biometric identifications. So many researches have been conducted on differentiating genuine signatures from forgeries. There could be multiple types of forgeries, such as random, simple or skilled(Hafemann, Sabourin and Oliveira, 2018). Weeding out the forged signatures is a huge task on its own. However it gets even more problematic if it were to be an offline handwritten signature.

This chapter will dive into the previous research findings on the above mentioned topics and further goes on to discuss the remaining research gap on these problems, the approaches and techniques used to acquire those knowledge.

Similar products and technologies

This chapter covers a breakdown of some existing level product solutions and some research undertaken for the features proposed solution with detailed explanation .

Facial Recognition

Many facial recognition systems were implemented, and other projects were proposed over the past few years.

One of them was a basic facial recognition system for security access and identification by Jeffrey S. Coffin and Darryl Ingram.This main purpose of this system was to allow users to get clearance access by using an authorized operator to enroll an image of the user through a facial scan and is compared in a database where each user Is given a personal identification number which is found in a particular location with:

*.Camera positioning information

*.Clearance data

*.Reference facial image scan(Incorvia, 2015)

The system is also capable of identifying a person wearing glasses or attempted disguises and can also detect and identify unwanted persons, such as known terrorists and fugitives.

Another holistic facial identification method by Kenneth Dong and Elena Dotsenko correcting the pose or lighting of the picture before the picture is compared with the stored images. This method makes use of:

*. Three-dimensional images with an original two-dimensional image by combining it with shape information and this picture is manipulated to change the pose and lighting characteristics used on the users' picture.

*. The three-dimensional picture will be converted back to a two-dimensional picture when in the process for an accurate recognition of a user(Ingram, 1999).

A facial recognition which was designed and implemented by M.Meenakshi makes special use of a digital signal processing prototype for facial recognition and verification. This system includes features in the previously mentioned systems, that is, capturing a picture of an individual in a sequence and checking for similar features to recognize and verify a person but, this process is done real time using the TMS320C6713 DSP (Meenakshi, 2013). The real time processing is done by a PC based system with algorithms based on MATLAB(Meenakshi, 2013). The proposed system's purpose is to reduce the size , increase speed and accuracy of recognizing and verifying a person.

Liveness detection systems designed to detect eye movement to recognize a live face from a photographed face is a relatively different approach with promising results. This approach uses 5 sequential face images to detect both eyes and to find the center of the eyes to extract the eye region from the face. Then the algorithm converts the extracted eye region into binary to

compare against the other captured image's eye region. Live face image would have higher variations when compared than the photographed images due to pupil movements and eye blinking (Hyung-Keun Jee, Jung and Yoo, 2008)

ID Verification

A recent study of identity card verification system which was developed by Chinapas et al. in 2019 which uses MTCNN which is a type of CNN (Convolutional Neural Network) for face detection as it had the best performance and had several models compared to the other face detection systems. A picture of a thai identity card was used for this purpose which contained an image of a face without any accessories such as glasses and headgears.

Afterwards for face comparison ArcFace(Additive Angular Margin Loss for Deep Face Recognition) was used which has the best accuracy over the other main face comparison systems (Dlib and Facenet) as mentioned in the study.

The system has 4 main steps such as:

1. ID card detection
2. Crop face by ratio
3. Face Detection
4. Face Comparison

Step 4 is achieved by comparing the image of the face in the ID and a picture(different) of the ID holder which is as well cropped by ratio.

From their study Chinapas et al. concluded that ArcFace was the best face comparison system for identity cards as it delivered the best results compared to other systems by detecting the face over scratched and shiny images.(Chinapas, Polpinit, Intiruk and Saikaew, 2019)

Signature verification

Many identification systems were developed these years, using different methods, different approaches and different technologies.

One of these was an Offline Signature Recognition and Forgery Detection using Deep Learning developed utilizing signatures as biometric features, by using Convolutional Neural Networks (CNN) for signature verification and Crest-Trough for forgery detection by Jivesh Poddar,

Vinanti Parikh and Santhosh Kumar Bharti. Having various steps in order to get more accurate results, steps such as:

- noise removal - to remove pixels unrelated to the signature
- scaling - to scale back the general space of the image
- centralization - to centralize the signature
- rotation - which places the signature at a zero degree angle for better accuracy (Poddar, Parikh and Bharti, 2020)

Another system created to detect forged signatures using Convolutional Neural Networks by Gideon et al. mention about four various type of forgeries executed which are:

- Simulation forgeries - if a forger has a sample of the signature to be forged
- Unknown/random/blind forgeries - if a forger has no or little insight of how the signature resembles, this is the simplest sort of forgery to recognize.
- Tracing forgeries - if a forger traces the lines of the legit signature onto the paper that needs to be signed
- Optical transfer forgeries - if a forger conveys a genuine signature using a photocopy machine, a photography, a scanner or any other method that enables the user to do so.

This system uses some steps as the previously mentioned system such as the noise removal and scaling but with two additional steps worth mentioning:

- RGB to Grayscale - convert any image color to grayscale to reduce the computational complexity of the digital image processing drastically
- Grayscale to Bitmap - the image file format is utilized for storing the digital image used later for comparison purposes (Gideon et al., 2018)

Another dynamic signature verification system which is based on one real signature by (citing). Focuses on training a model to verify a signature using only one given reference signature. Their strategy consists of duplicating the actual signature couple of times and training a model to verify the signature with each of those duplicated signatures. They train this model by using two methods:

*. The first method checks the strokes lognormal parameters (stroke wise)

*. The second method modifies their virtual target points(target-wise)(Diaz et al., 2018)

Research Gap

Signature verification

In most existing signature verification systems, it was noted that a user's signature input has a high intra-class variability, these are variations that occur between different inputs of the same class. Which means that signatures provided from the same user would have variations between samples. These variations are based on certain factors surrounding each user such as their age, health status, geographical location and their current emotional state. (Garhawal and Shukla, 2013).

This would be problematic to the signer as well, as the exact signature pattern should be placed, based on the initially registered signature. Even the slightest change in their signature would be denied. Since their handwriting patterns are not observed or taken into account. So, in order to eradicate this limitation, the proposed project involves capturing the dynamic information of these signature samples, these characteristics include its dynamically captured direction, stroke, pressure, and the shape of an individual's signature, So this can enable handwriting to be a reliable predictor of the individual's identity.

Another limitation was that there were not enough additional datasets available publicly in order to help train the systems to distinguish it against forgeries specifically. This would have not resulted in better performance in terms of accuracy, especially in the situation of skilled forgery (Hafemann, Sabourin and Oliveira, 2018).

However, as of now, more datasets under signatures are publicly available especially through online data science communities such as Kaggle. Usually containing two sets of information, one representing genuine signatures and the other on forged signatures. On average at least 1000 plus signatures were used to train the existing models, currently as of now 7000 plus signatures have been collected for the signature verification model, so with a large sample size, the solution can produce reliable results once the model has been trained. Therefore, a consistent number of datasets have been collected necessarily to help improve the accuracy and performance of our signature verification model.

Facial recognition

Most facial recognition systems alone are not capable of acknowledging an ‘actual’ face against a ‘spoof’ face. A face spoof attack is an attempt to get through a face recognition system, by disguising themselves as the original user, therefore gaining unauthorized access into the user’s device. The following spoofing techniques is done by substituting the original face through the use of a printed photo, eye-cut photo, video playback, or even a 3D mask (Souza et al., 2018).

Figure 2.1 Face Spoof Techniques (Shiranthika, 2019)

This was noted especially on smartphone devices which had a facial recognition feature. In order to overcome this security threat, a liveness detection system has to be implemented and work alongside facial recognition. With this system the user will have to perform a task while going through the Facial Recognition process, the task will require the user to perform a specific facial gesture. Once the following task is completed. (Chakraborty and Das, 2014).

Then only the user will gain authorized access. This would be used to determine if the input provided from the user is an actual face or not, based on the acted motion, such as facial movements over the eye area and mouth area. Therefore by considering the following measures, it can help reduce the chances of these face spoof attacks occurring, along with making facial recognition a safe approach.

Research on Approaches & Techniques

There are multiple researches on identity verification using facial recognition, identity document verification and signature verification. Most of these approaches are on deep learning networks to identify genuine characteristics of each verification method.

Signature Verification

Most of the existing research on signature verification is based on Convolutional Neural networks which are mostly used for visual imagery analysis using the image's structure. One research approaches this with three convolution neural networks with the image of the signature goes through back and forward several times to train the model which is then used to identify whether a given signature is genuine or not according to the images from the database (Gideon et al., 2018). Another research was done by using the Auto-Encoder algorithm which is based on unsupervised feature learning of the signature to improve the signature's variability compatibility for the system. This is done by considering the intensity of pressure and time of each position of signature which has two channels (Saffar et al., 2018). Another research was based on the Sigma-Lognormal Model which calculates the intrapersonal variability of the signature which improves recognizing the variability of the signature (Diaz, Fisher, Ferrer and Plamondon, 2018)

Face Recognition & Liveness Detection

Several researches on Facial Recognition based on Neural Networks, Principal Component Analysis, Linear Discriminant analysis and Support Vector Machines. Facial recognition is about extracting the features of the face to identify the person. This process has been done in several ways. Local Appearance based technique is about analysing critical parts of the face such as nose, mouth and eyes. The Key Point based technique is about analyzing geometric features of the face such as distance between the eyes and nose, etc.. Beside those local feature based approaches there is also the Holistic approach which is about representing the face image as a matrix of pixels which will then be analysed to recognize the facial features. And there is also the Hybrid approach which combines both of the ways to improve the performance and accuracy of facial recognition systems.

Identity Document Verification

Most researches are mostly based on Classification Algorithms since the document only needs to be a valid one. The information is then extracted from the Document and compared with the information from the database to verify it. In one of the researches the document verification process classifies a set of features which describe the visual layout and information of the Identity Card image. After checking the validity of these extracted features, the system will then produce an output of the authenticity of the given Identity Card image(Castelblanco et al., 2020).

Considering the previous research on approaches on each of the verifications, the solution needs to have a high accuracy rate of successfully verifying each component. For the signature verification, a convolution network will not be enough to improve the accuracy. It may needs to be combined with a clustering algorithm or will have to produce a machine learning algorithm which will trace the way of writing the signature from an image which will then be analyzed through with a clustering based and convolution neural network based algorithm to increase the accuracy as well as to decrease the Error rate of accepting dynamic signature characteristics. For the face recognition method, a combined machine learning algorithm which takes advantage of both local features technique and the matrix based technique will be more appropriate as it will increase the accuracy. For the identity document verification, a traditional image classification method will be sufficient as it only needs to identify whether the characteristics of the identity card is valid or not which will then the information will be extracted through an OCR process to be verified with the database information.

Chapter Summary

In the literature review team have explained details about the previously done researches on facial recognition/liveness recognition and signature recognition using various approaches. The most common approach among the researchers was to use Convolutional Neural Networks to identify signatures. When it comes to facial recognition and liveness detection the most favored techniques were approaches such as Support Vector Machines and Linear Discriminant analysis.

The team is proposing dynamic information analysis in signatures to improve the accuracy of the identification process in the signature identification component. And to use facial expression analysis and liveness detection to identify doctored images to improve the facial recognition component of the system.

References

Diaz, M. et al. (2018). Dynamic Signature Verification System Based on One Real Signature. IEEE Transactions on Cybernetics, 48 (1), 228–239. Available from https://doi.org/10.1109/TCYB.2016.2630419.

Jerome Gideon, S. et al. (2018). Handwritten signature forgery detection using convolutional neural networks. *Procedia Computer Science*, 143, 978–987. Available from https://doi.org/10.1016/j.procs.2018.10.336.

Saffar, M.H. et al. (2018). Online Signature Verification using Deep Representation: A new Descriptor. x, 1–10. Available from http://arxiv.org/abs/1806.09986.

Poddar, J., Parikh, V. and Bharti, S.K. (2020). Offline Signature Recognition and Forgery Detection using Deep Learning. Procedia Computer Science, 170 (2019), 610–617. Available from https://doi.org/10.1016/j.procs.2020.03.133.

Chinapas, A. et al. (2019). Personal Verification System Using ID Card and Face Photo. International Journal of Machine Learning and Computing, 9, 407–412. Available from https://doi.org/10.18178/ijmlc.2019.9.4.818.

Chakraborty, S. and Das, D. (2014). An Overview of Face Liveness Detection. *International Journal on Information Theory*, 3 (2), 11–25. Available from https://doi.org/10.5121/ijit.2014.3202.

Souza, L. et al. (2018). How far did we get in face spoofing detection? *Engineering Applications of Artificial Intelligence*, 72, 368–381. Available from https://doi.org/10.1016/j.engappai.2018.04.013.

Shiranthika, C. (2019). Face Spoof Detection. Bio-metrics is the giant in utilizing… | by Chamani Shiranthika | Data Driven Investor | Medium. Available from https://medium.com/datadriveninvestor/face-spoof-detection-e0d08fb246ea [Accessed 17 November 2020].

Meenakshi, M. (2013). Real-Time Facial Recognition System—Design, Implementation and Validation. *Journal of Signal Processing Theory and Applications*. Available from https://doi.org/10.7726/jspta.2013.1001.

Castelblanco, A. et al. (2020). Machine Learning Techniques for Identity Document Verification in Uncontrolled Environments: A Case Study. 271–281. Available from https://doi.org/10.1007/978-3-030-49076-8_26.

Tan, X. et al. (2010). Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model BT - Computer Vision – ECCV 2010. In: Daniilidis, K. Maragos, P. and Paragios, N. (eds.). 2010. Berlin, Heidelberg: Springer Berlin Heidelberg, 504–517.

Hafemann, L.G., Sabourin, R. and Oliveira, L.S. (2017). Offline handwritten signature verification — Literature review. *2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA)*. 2017. 1–8. Available from https://doi.org/10.1109/IPTA.2017.8310112.

Hyung-Keun Jee, Jung, S.-U. and Yoo, J.-H. (2008). Liveness Detection For Embedded Face Recognition System. Available from https://doi.org/10.5281/ZENODO.1060812 [Accessed 22 November 2020].