

Hindi Signature Verification using Data generation with Generative Adversarial Networks

*A project report submitted in partial fulfillment of the requirements for
B.Tech. Project*

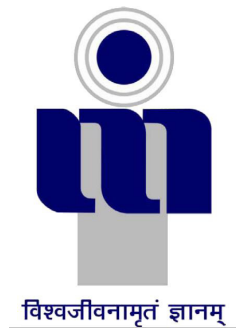
B.Tech.

by

Jatin Kasera (2018IMT-042)

Under the Supervision of

Prof. Rajendra Sahu



**ABV INDIAN INSTITUTE OF INFORMATION
TECHNOLOGY AND MANAGEMENT
GWALIOR-474 015**

2021

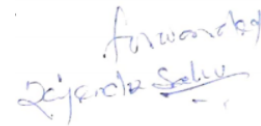
CANDIDATES DECLARATION

I hereby declare that this work presented in the report, titled **Hindi Signature Verification Using Data Generation with Generative Adversarial Networks**, in partial fulfilment of the requirement for the award of the Degree of Bachelor of Technology and presented to the institution is an authentic record of my own work carried out during the period *June 2021* to *October 2021* under the supervisory of **Prof. Rajendra Sahu**. I also included a reference to the text(s)/figure(s)/table(s) from which they were derived.

Date: 23-10-2021

Signatures of the Candidate

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

A handwritten signature in blue ink, reading "Rajendra Sahu", with the word "forwarded" written above it.

Date: 23-10-2021

Signatures of the Research Supervisor

ABSTRACT

This report is based on Hindi Signature Verification using Data generation with Generative Adversarial Networks. Handwritten Signatures are one of the most prominent bio-metrics to authenticate documents (in banks, institutes). The effectiveness of this issue resides in digital authentication and human authority. Because of the huge increase in the quantity of documents signed, the frequency of frauds in signatures has increased significantly.

Contemporary studies show that banks experience about 900 million dollars of check fraud every year. In addition, 22% among all cases are caused by signature deception. That forces companies to make use of extensive historical transaction data, which can replace traditional visual detection, to uncover patterns of fraud signatures by building new algorithms. Despite extensive research in this sector, identification is limited to the English signature, with no progress in languages such as Hindi, Chinese, and so on. Because the existing models only function on short data sets, we would like to do research on Hindi signature fraud detection using GAN to produce huge data sets and apply genuine and Forged detection on such data sets. The generative approach is a type of unsupervised machine learning method that includes itself identifying and predicting the regularities and irregularities or patterns in the supplied input data so that the model could be useful in generation of new images. SVMs can be used for verification. An effective signature verification system must be built, capable of detecting all forms of forgeries using trustworthy, specialised algorithms.

Keywords: - Signature identification, Image processing, Support Vector Machines, Generative Adversarial networks.

ACKNOWLEDGEMENTS

I am extremely grateful to **Prof. Rajendra Sahu** for allowing me the freedom to operate and explore with ideas. I'd like to take this opportunity to express my heartfelt gratitude to them not only for their academic guidance, but also for their professional values in my project and consistent support, as well as esteem and motivating sessions that proved extremely beneficial and were instrumental in instilling self-assurance and trust. The current work has been nurtured and blossomed mostly as a result of their valuable direction, recommendations, astute judgement, constructive comments, and an eye for excellence. My mentor constantly answered all of my questions with a smile, gratitude, and tremendous patience, never making me feel inexperienced by always listening to my ideas, recognising and refining them, and allowing us a free hand in the project. Only because of their tremendous enthusiasm and helpful attitude has the current effort progressed to this point.

Finally, I want to express my gratitude to our Institution and colleagues, whose constant encouragement helped to revive my spirit, concentrate our attention and energy, and assisted us in making this research.

Date: 23-10-2021

Signatures of the Candidate

TABLE OF CONTENTS

ABSTRACT	2
LIST OF FIGURES	4
1 INTRODUCTION AND LITERATURE SURVEY	7
1.1 Introduction	7
1.2 Motivation	8
1.3 Literature Survey	9
1.4 Objective	10
2 METHODOLOGY	12
2.0.1 Data Collection	12
2.0.2 Pre-Processing	13
2.0.2.1 Noise Abatement	13
2.0.2.2 Binarisation	13
2.0.2.3 Scaling	14
2.1 Generative Adversarial Network	14
2.1.0.1 Generator	15
2.1.0.2 Discriminator	15
2.1.0.3 Loss Function	16
2.2 Extraction of Features	16
3 RESULTS AND CONCLUSION	19
3.1 Results	19
3.2 Conclusion	20
REFERENCES	20

LIST OF FIGURES

2.1	Some Collected Sample Signatures	13
2.2	Grey-Scale Image	13
2.3	Converted Binary Image	14
2.4	Basic Block Diagram of GAN	14
2.5	Basic Block Diagram of Generator	15
2.6	Basic Block Diagram of Discriminator	16
2.7	Vowels and Consonants of Devanagiri(Hindi) script	17
3.1	Authentic and Fake Signs after training on GAN	19
3.2	After gradient method, authentic Sign confused as fake sign	20
3.3	After gradient method, fake Sign confused as authentic sign	20

ABBREVIATIONS

GAN	Generative Adversarial Network
DCGAN	Deep Convolutional Generative Adversarial Network
SVM	Support Vector Machines
CNN	Convolutional Neural Network

CHAPTER 1

INTRODUCTION AND LITERATURE SURVEY

1.1 Introduction

Intensive studies have been undertaken on signature verification during the past few years due to considerable financial applications. Authentication-related concerns may be identified and verified by signatures. According to [1] permitting methods are split in 2 classes:

- Online methods, that uses dynamic processes such as digitized signature to take account of speed and pressure utilising smart algorithms.
- Offline approach, signature on paper is signed and scanned to transform it into a digital signature using the optical scanner.

In this thesis we concentrate on offline control systems that have a significant advantage since they have more practical applications. in financial organisations such as banks, etc.

Despite significant progress in the area of offline verification of English signs. However, because signatures can be signed in other languages, such as Hindi,etc we should do a comprehensive investigation in this field. As a result, Hindi signature recognition and validation would be considered a significant solution to reducing signature frauds in India.

Nowadays, whether in the banking or business sectors, a handmade signs is among few of the most frequently acknowledged personal qualities for confirming identity. Due to a lack of education and expertise, many from the lowest social classes choose to sign their names in free handwriting. As a result, in certain circumstances, these types of signatures are simple to forge. Four sorts of forgeries are available in this instance [2].

- **Simulation/Simple Forgery** : A type of forgery in which the forger has a sample of the falsified signature. The quality of a simulation is determined by amount of practise done by the forger in order to commit the real forgery, the ability of the person committing fraud, and the amount attention to detail given by the fraudster while committing fraud. Unskilled and skilled forgeries are classified based on the forger's experience.
- **Blind Forgery** : This is when the fraudster has no notion what the faked signature would be in appearance. This is the most difficult sort of forgery to identify since it does not have the appearance of a genuine signature. Many signature attributes might differ even when two signatures are made by the same person. As a result, spotting a fraud becomes a complicated task.
- **Tracing** : The third sort of forgeries is tracing. It is done by arranging the reference document and the concerned document up to the light and tracing the lines of the reference sign over onto questioned document with a pen. Tracing can also be accomplished by using a sharp brush on the questioned document to create the perception of the model signature in the paper. This image is then filled in with a pen to produce the look of the models signatures. If the forger's model signature cannot be identified, this form of forgery might be hard to spot from a replica.
- **Optical Transmission** : It is a method of transferring an authentic signature onto a document using a xerox, scanner, replica machine, or photography. An examiner cannot definitively recognise a signature as authentic in this form of forgery unless having the Authentic to compare it against.

To tackle both the problem of acquiring a decent feature representation for signatures and the issue of using SVM classifier, we propose a system for training the abstractions directly from the sign pictures using the deep neural networks. We suggest, in particular, a unique formulation of the issue that integrates knowledge about competent sign fraud from a subset of users through the application of a cross learning technique. The idea is that the model can itself learn visual (images) information in signs data that distinguish actual(real) signs from duplicate forgeries.

1.2 Motivation

With the course of time, there has been a lot of work done in the domain of offline verification of English signatures. Numerous research papers on English signs validation have been presented. But, there is no such development when it comes to other languages like English. The main concern is of unavailability of such Hindi signature data sets to train the models on. Therefore a data set has to be created for Hindi signs

too, for this purpose we use GAN to increase the size of our data set and gain proper insights of the results to be proposed by the model.

As a result, the basic concept of signature identification and verification can be proposed by treating the signature as an image and extracting each pixel. Signature verification has a wide range of applications, particularly in the financial sector, where check fraud and bank withdrawals have increased in the last several years.

1.3 Literature Survey

As proposed by [1], the signature verification is practically divided into 2 methods of-line and online. Online methods that checks on signatures were proven to achieve substantially better verification results than off-line methods, since there is a much loss of dynamic data in off-line mode. Online method will require more security of the system from online attacks. Offline systems have a significant advantage since when signatures are produced, this method doesn't involve use of any specialised hardware. Furthermore, because of financial applications in banks, off-line verification is more realistic in use.

According to [3], the examination of human signatures focuses in particular on improving the interaction between people and technology. Thus this process must be reliable to a better extent because of its vast applications in financial domains such as banks, institutions etc., as the years passing by number of Signature frauds has been increasing at such a rapid rate.

As suggested by [4] offline signature verification is concerned with the signature as static data formats. The main concern in offline signature verification can be divided into 2 types:

1. **Identification:** it entails detecting whether a signer is already a user among the possible Database.
2. **Verification:** this is done after identification, if a signer is a user, then does its signatures matches with the one in Database.

Signature are often misunderstood as just group of words and letters but they are more than that. As mentioned in [5], signatures are regarded as a image with a unique property like having pixel distribution and every signature has distinct style of writing, thus they may have different pixel distribution.

[6] introduced a clustering-related approach to this problem. This process involves use of filtration methods to eliminate noise, image is further pre-processed to dilute the images of the signature. The Region of interest is identified and its is matched with the current signature and original signatures. If they have sufficient similarity score

then it is real otherwise forged. But this method was also implemented only on English signatures.

In the field of off-line methods, when it comes to western signatures, tremendous research work has been carried out. [7] established a successful approach for verifying and identifying off-line signatures. This method includes structural feature extraction from contour of the signature. Signatures can be written in various languages and a comprehensive study in this field is necessary. A number of published works can be found on Western signatures and only some studies on signatures written in Arabic, Chinese, Persian, Japanese have been carried out like [8], but not efficient as the size of data set used to train was much less.

Significant work related to offline Hindi Signature Validation has been done by [9], they collected data set from their research students and applied gradient feature techniques using SVMs. In the [10], they proposed the same solution for multi language signature validation system, first they identified the language of the signature by using Devnagiri lipi there after feature extraction techniques were used. But the most drawback of this approach was manual generation of dataset. So this problem can be reduced by using GAN to generate similar images using the available data set. A large Data Set has to be used to provide better results.

We propose that training of GANs ([11]) and re-use of sections of the discriminator and generator networks should be one strategy to generate good representation of the image. In tasks such as Image production GANs now show excellent results.

As proposed in [12] similar images can be generated using DCGANs on available dataset, DCGAN is Deep Convolutional Generative Adversarial Networks, is used here to stabilize the GAN models as GANs are considered unstable, Convolutional GANs can be used to get efficient results.

1.4 Objective

Financial institutions such as banks etc. and companies recognise the main way in which transactions are authenticated. Cheques are signed, contracts and documents are permitted, transactions of credit cards are validated and verified using signatures. With availability and numbers of signed documents enormously expanded, this in turn causes the spike cases related to signature forgery. Extensive research has been made but only in English signatures, but there are lot of people in India, still uses Hindi Signature as their authentication method.

This project mainly focuses on using offline signature validation methods on Hindi Signature data sets. The unavailability of large data set of Hindi signature data to train model on, can be solved by studying Generative Advarasial Networks.

The following are our primary contributions:

- In a Writer Independent pattern, we propose formulas for learning features for offline sign verification and identification. We present a rigorous method under which all the design judgements are based using from a set of predictors composed of a different set of users.
- The project proposes a unique method that uses competent frauds from a collective units of signs data to guide the feature cognitive development, using a multi-task template to jointly optimise the model to distinguish between users (tackling arbitrary frauds), and to distinguish between legitimate ones and competent frauds.
- To gain better insights of data, GAN is used to increase the size of the available dataset for Offline Hindi Signature Verification.
- We offer a clear assessment of the learnt representations, demonstrating that authentic signs and competent replicas of Hindi Signs can be distinguished in separate sections of the feature set.

CHAPTER 2

METHODOLOGY

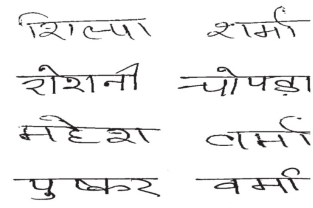
Many signature attributes might differ even when two signatures are made by the same person. As a result, spotting a fraud becomes a complicated task. Offline signature validations takes input of the signature images, this signature images might contain some noise, so filtration has to be done on this images, so that it doesn't affect the further process to be carried out. The data set available to us has very limited size, thus its size has to be increased to get better results.

The written signature is a based on behavioural characteristics of the person rather than physiological characteristics of the users signature. Because signs of a person can change with passage of time, the validation and identification of the signature may take a lengthy time, resulting in increased errors in some circumstances. Inconsistent signatures result in greater false accept rates for those who do not sign consistently.

With the recent developments in Deep Learning, Generative Adversarial Networks have proven a better choice to generate similar images as our signature data is not considered as group of words letters but images. For our task, we have used a Studied Generative Adversarial Network. Following is the description of the methodology followed and the complete description of the models that can be used and their implementation details.

2.0.1 Data Collection

Handmade signs of Hindi script are captured, and some distinguishing characteristics are retrieved, in order to construct a base of knowledge for each individual. A standardised sign database for each subject is required for evaluating the performance of the sign authentication scheme and comparing the results acquired using different technologies on the same database. Initially some authentic and fake signs were collected.



शिल्पा शर्मा
रीशनी चौपड़ा
महेश वर्मा
पुष्कर वर्मा

Figure 2.1: Some Collected Sample Signatures

2.0.2 Pre-Processing

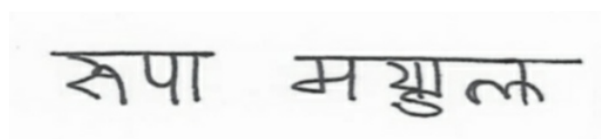
The Signature used by the model is to be in digital images format. Thus signatures are collected by signing on fixed size of paper then scanning it using any scanning device. This may contain some irregularity which has to be removed by filtration and discarding images which are not useful.

2.0.2.1 Noise Abatement

Noise is the outcome of errors induced by many sorts of acquisition processes, resulting in image pixels that do not correspond to genuine values. The picture obtained from a lens includes film grains, which are a bit noisy, and it might be generated by damaged when it is fed into the scanners. Furthermore, image dissemination via electronic means can cause distortion. The analyst is unaware of any additive noise present in the signature image, and its amount is unknown. To improve the noise separation process, a known type of noise is injected to the gray-scale image in a very small amount. This increases the threshold of the noise and hence can be filtered using a filter.

2.0.2.2 Binarisation

Initially Sign images are collected in unique 256 grey-scale level and 360 dpi and placed in specific format of images known as TIFF. First the digitized image is transformed into binary image, this further converted into two tone images, Which can be used for further process. Gray - scale signs images are turned to bitmap signs images, and image file formats are used to preserve this digital images . Below figures depicts the outcome of this operation:



रूपा मशुल्

Figure 2.2: Grey-Scale Image

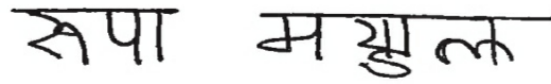


Figure 2.3: Converted Binary Image

2.0.2.3 Scaling

The model must be able to ensure good performance irrespective of the angle and size of the signs. It is critical that the model should be not responsive enough for the signs image restoration. The matrix of image is adjusted to conventional scale, which would be 256 at 360 dpi .

2.1 Generative Adversarial Network

The pre-processed image is passed through GAN model to increase the size of the available dataset. GANs is an algorithmic design composed of 2 neural networks, which are mutually competitive (hence "adversarial") in the generation of replicated sample data that can be passed on for real data. The GAN is an unsupervised form of machine learning, whereby the patterns or the regularities of the data input are discovered naturally, so that the model can be used to produce or generate new images (here images but can be other data) which could be taken from the original input image data set. various other applications of GAN is generation of audio and video signals.

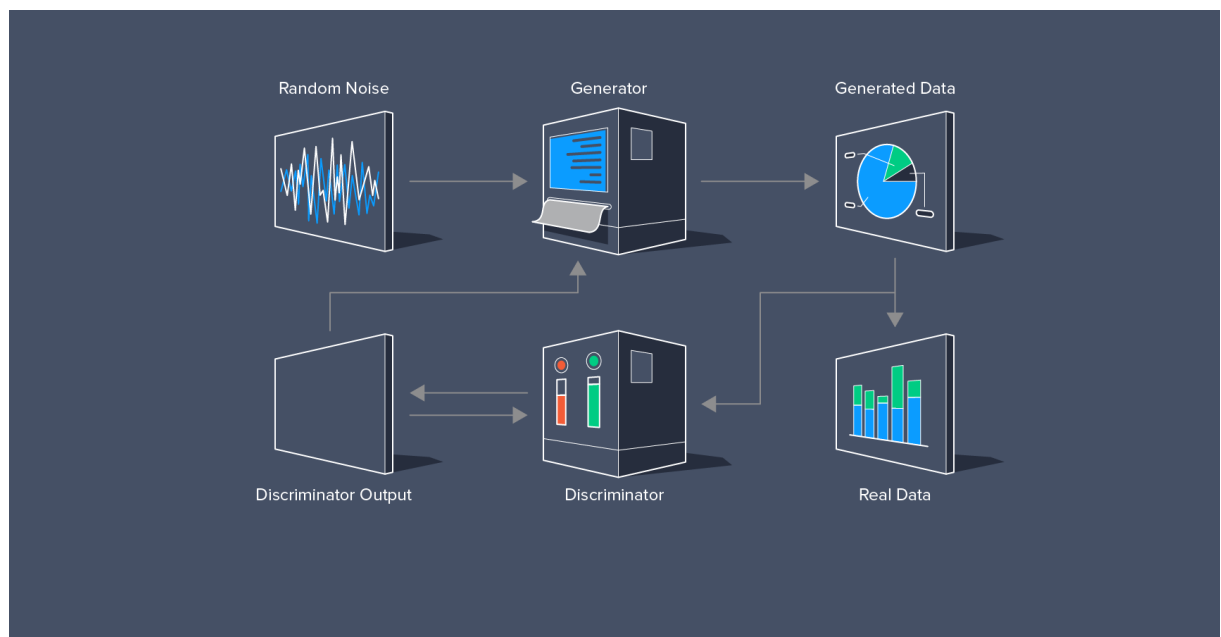


Figure 2.4: Basic Block Diagram of GAN

2.1.0.1 Generator

The generator is analogous to the heart of the architecture. It is a model that is used to produce new similar data like images, and it is invest in order to obtain really high performance at the end of the training process. The purpose of the generator is to be able to generate synthetic instances from a given input. So, for example if we train it with images of dogs then it will generate similar images to dogs, the generator will perform certain computations and return a realistic representation of a new dog which will look real. So, ideally, the generator will not return the same dog on running every time, so the input will be distinct sets of random numbers, known as a noise vector, to ensure it can generate fresh realistic images every time.

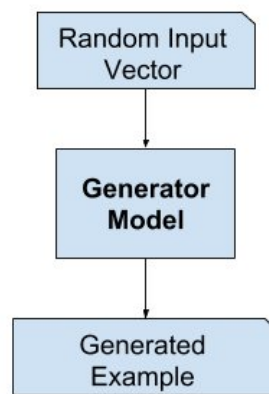


Figure 2.5: Basic Block Diagram of Generator

2.1.0.2 Discriminator

The discriminator is a sort of classifier whose goal is to distinguish between actual and created data that is real or fake. Classifiers aren't just for selecting image data, it can be video, audio or anything else here. As a result, the discriminator is a form of classifier that learns to estimate the likelihood of a given example being real or fake using input data such as images' pixels values. The discriminator's output probabilities assist the generator in learning to provide better samples over time.

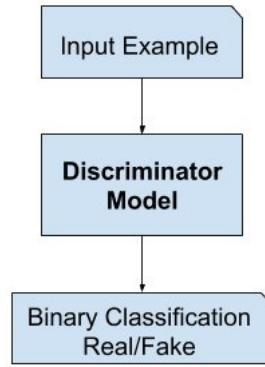


Figure 2.6: Basic Block Diagram of Discriminator

2.1.0.3 Loss Function

The loss function of a generative adversarial network is:

$$E_x[\log(D(x))] + E_z[\log(1 - D(G(z)))] \quad (2.1)$$

where

- $D(x)$ is discriminator's output value for a given x .
- x is a real sample .
- z is a an instance of random noise.
- E_x means the probable value over all x .
- $D(G(z))$ is the probability given by discriminator's if a forged sample is genuine.
- $G(z)$ is the output of the generator for a given input z
- E_z means the expected value over all z .

The main objective of generator to reduce the value of the loss function, which equates producing samples that look like real ones. On the other hand, the discriminator tries to increase the loss function.

2.2 Extraction of Features

The images from the GAN model is further processed to detect the authentic and replica of signs. This task is mainly accompanied by using the extraction of features. But before extracting features, the devanagiri script's properties must be studied carefully. In Devanagiri, a Hindi script, in which the specific direction of writing is from the

left to right, in Hindi script, there is no such thing as upper characters and lower case characters. The signs in this script has 3 zones lower, upper and middle. The vowels does not modify the middle zone. Hindi script has basic 50 chars. The below image is descriptive image of vowels and consonants in devanagiri(Hindi) script.

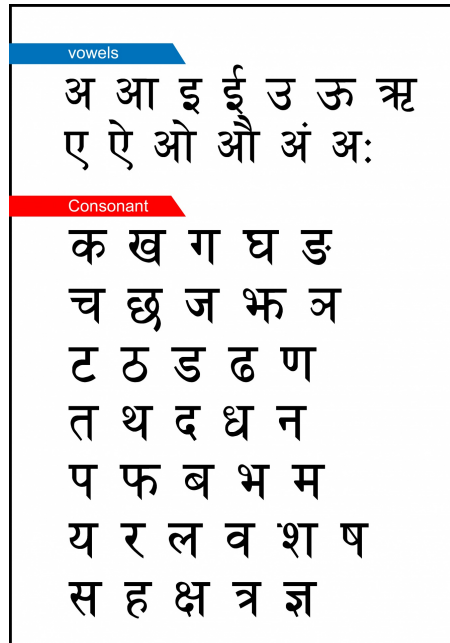


Figure 2.7: Vowels and Consonants of Devanagiri(Hindi) script

The extraction of characteristics from an image plays a vital role in any recognition task. For this purpose Gradient method of extracting characteristics is deployed. The Gradient method of extracting characteristics can be summarised as follows: The handwritten element's grey-scale local-orientation histogram is utilised to obtain 576-d characteristics.

The steps followed to generate a 576-d based on gradient feature vector.

- **Step 1:** The images from GAN is filtered 4-times using mean filters of 2×2 .
- **Step 2:** The output of the Step 1 i.e. grey scaled sign images is further gone through normalization till the mean of the grey images scale equals to 0 and max value is 1.
- **Step 3:** The images after going through normalization is further divided into blocks of size of 17 into 7. The size of block is determined empirically, balancing the trade-off between correctness and complication. The grey scaled sign image is turned into a two-tone sign image. This will result in removal of any extraneous additional details from the sign images.
- **Step 4:** To create the gradient sign image, a filter of Roberts is applied to the system. The gradient's arc tangent (path of gradients) is gone through fragmented

into 32 orientations, and the gradient's intensity is compounded with each of the quantified orientations. The Gradient ($f(A,B)$) strength is specifically defined:

$$f(A, B) = \sqrt{(\Delta a1)^2 + (\Delta b1)^2} \quad (2.2)$$

and the orientation of gradient is:

$$\Theta(a, b) = \tan^{-1} \frac{\Delta a1}{\Delta a2} \quad (2.3)$$

in this :

$$\Delta a1 = g(a + 1, b + 1) - g(a, b) \quad (2.4)$$

$$\Delta b1 = g(a + 1, b) - g(a, b + 1) \quad (2.5)$$

The $g(a,b)$ is the value of grey scaled sign image at point a,b .

- **Step 5:** The 17 into 7 is converted to block size of 9 into 4 across 16 orientation, thus $16 \times 9 \times 4 = 576$.

CHAPTER 3

RESULTS AND CONCLUSION

3.1 Results

The extracted features were passed through SVM classifiers , first the sample training and testing was done on small dataset containing authentic and replica of signatures collected and passed through GAN.

Table 3.1: No. of Authentic and Duplicated Signs used for Sample Training

	Authentic Signatures	Duplicated Signatures
Training	15	21
Testing	12	11

But this is size of the basic training and testing. But the actual size on which the model trained were 860 real signs and 1040 fake signs to begin from a public dataset. The signatures were passed through GAN model first it will generate fake images that will be used in further process.

Hindi Signatures	
Genuine Signatures	Forged Signatures
सुरेश वाजपेयी	सुरेश वाजपेयी
प्रदीप वर्मा	प्रदीप वर्मा
विकास मोदी	विकास मोदी
विवेक मटेश्वरि	विवेक मटेश्वरि

Figure 3.1: Authentic and Fake Signs after training on GAN

To check the performance of this models, 2 types of errors are exists first one is False Rejection, it is also known as Type-1 error. This is measured by amount of authentic signatures classified by the model as fake signatures. The rate at which the model does this work is known as False Rejection Rate, FRR.

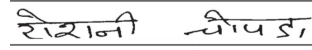


Figure 3.2: After gradient method, authentic Sign confused as fake sign

Second one is False Accepted, it is also known as Type-2 error. This is measured by amount of fake signatures classified by the model as authentic signatures. The rate at which the model does this work is known as False Acceptance Rate, FAR.



Figure 3.3: After gradient method, fake Sign confused as authentic sign

3.2 Conclusion

The Hindi Signature verification system is useful for many practical areas like finance, institutional etc. So the offline verification has to be done at greater extent. We have tested gradient extraction method. But other methods etc can be used for extraction, but they will have more errors. The Dataset size issue can be resolved by using GAN. But in future, a large public dataset can be created for this purpose and modify the overall performance of the system.

REFERENCES

- [1] S. Madabusi, V. Srinivas, S. Bhaskaran, and M. Balasubramanian, “On-line and off-line signature verification using relative slope algorithm,” 04 2005, pp. 11 – 15.
- [2] S. J. Gideon, A. Kandulna, A. A. Kujur, A. Diana, and K. Raimond, “Handwritten signature forgery detection using convolutional neural networks,” *Procedia Computer Science*, vol. 143, pp. 978–987, 2018, 8th International Conference on Advances in Computing Communications (ICACC-2018).
- [3] M. Ferrer, J. Alonso, and C. Travieso, “Offline geometric parameters for automatic signature verification using fixed-point arithmetic,” *IEEE transactions on pattern analysis and machine intelligence*, vol. 27, pp. 993–7, 07 2005.
- [4] I. Pottier and G. Burel, “Identification and authentication of handwritten signatures with a connectionist approach,” vol. 5, 07 1994, pp. 2948 – 2951 vol.5.
- [5] R. Plamondon, “On-line and off-line handwriting recognition: a comprehensive survey. iee trans pattern anal mach intell (t-pami),” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, pp. 63–84, 01 2000.
- [6] S. Biswas, T.-H. Kim, and D. Bhattacharyya, “Features extraction and verification of signature image using clustering technique,” *International Journal of International Journal of International Journal of Smart July*, vol. 4, 01 2010.
- [7] S. Armand, M. Blumenstein, and V. Muthukkumarasamy, “Off-line signature verification using an enhanced modified direction feature with single and multi-classifier approaches,” *IEEE Computational Intelligence Magazine*, vol. 2, pp. 18–25, 2007.
- [8] S. Pal, M. Blumenstein, and U. Pal, “Automatic off-line signature verification systems: A review,” *International Journal of Computer Applications*, vol. 14, pp. Pages 20–27, 01 2011.
- [9] —, “Hindi off-line signature verification,” 09 2012, pp. 373–378.

- [10] S. Pal, U. Pal, and M. Blumenstein, “Hindi and english off-line signature identification and verification,” vol. 174, 01 2012.
- [11] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, “Generative adversarial nets,” in *Advances in Neural Information Processing Systems*, Z. Ghahramani, M. Welling, C. Cortes, N. Lawrence, and K. Q. Weinberger, Eds., vol. 27. Curran Associates, Inc., 2014.
- [12] A. Radford, L. Metz, and S. Chintala, “Unsupervised representation learning with deep convolutional generative adversarial networks,” 2016.