# Generating Digital Signature using Facial Landmark Detection

Chittaranjan Pradhan, Debanjan Banerjee, Nabarun Nandy and Udita Biswas

***Abstract*—Information security has developed rapidly over the recent years with a key being the emergence of social media. To standardize this discipline, security of an individual becomes an urgent concern. In 2019, it is estimated that there will be over 2.5 billion social media users around the globe. Unfortunately, anonymous identity has become a major concern for the security advisors. Due to the technological advancements, the phishers are able to access the confidential information. To resolve these issues numerous solutions have been proposed, such as biometric identification, facial and audio recognition etc prior access to any highly secure forum on the web. Generating digital signatures is the recent trend being incorporated in the field of digital security. We have designed an algorithm that after generating 68 point facial landmark, converts the image to a highly compressed and secure digital signature. The proposed algorithm generates a unique signature for an individual which when stored in the user account information database will limit the creation of fake or multiple accounts. At the same time the algorithm reduces the database storage overhead as it stores the facial identity of an individual in the form of a compressed textual signature rather than the traditional method where the image file was being stored, occupying lesser amount of space and making it more efficient in terms of searching, fetching and manipulation. A unique new analysis of the features produced at intermediate layers has been applied. Here, we opt to use the normal and two opposites' angular measures of the triangle as the invariance. It simply acts as the real-time optimized encryption procedure to achieve the reliable security goals explained in detail in the later sections.**

***Index Terms*—CDNU Algorithm, Encryption, Facial Landmarks, Huffman Coding, Optimization.**

## I. Introduction

DIGITAL signature is used for the authenticity of the digital media. This has been considered as the solution to tampering and impersonation of the digital communications. To get the origin evidence, identity and status of digital content, digital signatures can be used. But here the idea of digital signature is used in a different way. The attempt is taken to use the created digital signature as a sign of presence of authentic person in the computer network (and can be extended further). A digital signature is basically based on public key cryptography [1]. Moving on to the next term- our faces has certain fixed features or landmarks like the eyebrows, jaw-line, lips, nose-line etc. Identifying and marking them out from an image is referred to as Facial Landmark Extraction [2]. In order to identify the landmarks, a classifier is used which is made up of certain underlying rules trained over a large set of images. Here the features are outlined by 68 points (as shown in Fig. 1). But before the landmarks are being extracted the face has to be identified first. In order to do this a separate classifier with a different set of rules needs to be trained to identify the face first. Different algorithms are available to prepare both the above mentioned classifiers. Here we will be dealing only with frontal face so classifier needs to be trained accordingly.

Fig. 1. Magnetization

Smile is one of the human expressions. So we can easily detect a smile in an image if we separately create a classifier for smiles. The detection of smile, face and facial landmarks with the help of respective classifiers can be done with a library available called OpenCV 3.0. This library would help us in incorporating the classifiers and detect face, facial landmarks and smile in real time. Moreover it also enables us to operate on the gained data. Finally, encryption technique is the process of converting the readable message to the unreadable format so that only the authorized people/systems can access the content [3].

The motivation for this work is that with the digital transformation people are connected through internet and share and exchange ideas, services and goods. In most of the cases to establish your uniqueness in the network or service providing website you need to create an account and remember usernames and passwords. This method give rises to two problems: (i) huge number of fake accounts with fake details can be created, (ii) if the details are somehow leaked there no

Chittaranjan Pradhan is with School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, India (e-mail: chitaprakash@gmail.com).

Debanjan Banerjee is with School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, India (e-mail: debanjan.banerjee98@gmail.com).

Nabarun Nandy is with School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, India (e-mail: nabarun286@gmail.com).

Udita Biswas is with School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, India (e-mail: ishabiswas@gmail.com).

978-1-5386-7595-3/19/$31.00 ©2019 IEEE

way to identify whether the real user is present or not. But our method would considerably reduce both. Our method has another advantage over the methods using facial detection for security which is, once the unique signature is created and registered then the images of faces of the person would not be required to store in the system or in database. Whenever the person wants to log in he would just have to scan his face which would create the signature and match whether that exists or not. This would considerably lessen the requirement for storage, databases can be easily transferred and adding to it is the finer security.

Section II provides the work already done in this domain. The proposed algorithm is presented in section III. Section IV gives the result analysis conducted by considering the CDNU algorithm. The conclusion has been given in section V.

## II. Related Work

The use of social media is increasing day by day. From last few decades security has become the major concern to the entire world. As the barriers has become virtualized to secure individual accounts and private data within it of employees or customers of corresponding organizations such as social networking sites, e-banks, online shopping enterprises on the internet, biometric verifications in terms of facial image recognition has been the topic of research in this paper. Diving into the field of facial image recognition, the first challenge has been to eliminate storing of images into huge databases that were earlier being done for facial id verification purposes. Images were either being stored in databases or in file systems with the path being stored in databases. Due to the increased use of multimedia content over the social media, the storage cost in database has increased; which may affect the database performance.

Minimization of database overhead has been achieved by storing facial features extracted out of images instead of storing image files. The process of image recognition and consequently extracting facial features has been researched upon greatly in the past. Along with the conventional facial recognition techniques; fuzzy logic and neural network can be combined for increasing the rate of recognition [4, 5]. Due to the ambient light and position of head, there is a reduction of performance. To resolve such problems, higher feature sets have been obtained. There are two kinds of pre-information used for facial recognition- semantic information and geometric/landmark information [6]. Our work comes under the later domain. Face landmarks consist of two tasks: face detection and facial landmarks [7, 8]. The aim of this paper is in detection of facial components by placing the landmarks on each component. In the literature study, the highest accuracy has been obtained by using 22 landmarks with an accuracy of 90.28% [5, 8]. Due to the advancements in deep learning concept, a new approach has been developed by using 68 landmarks with an accuracy of 93.88% [5, 9]. Lately a Distance and Slope method was applied on only 22 landmark points and was able to achieve 94.60 percent accuracy. The idea in this paper is to work on 68 landmark points and include larger number of data sets using the CDNU algorithm described later, which gives a more accurate result.

The second challenge has been to generate a digital signature uniquely identifying an image from the extracted facial feature dataset. This digital signature has been created for the following purposes- firstly to hash out the data sets for faster access from the database, secondly to compress the large number of numeric data that is being generated upon extraction of the features. Digital signature helps in maintaining the authenticity, integrity and non-repudiation of digital content.

Huffman coding algorithm is the proposed algorithm for signature creation in this paper. It is a lossless data compression technique which creates an authenticated and unique numeric value from the features extracted. It not only reduces the database size but also is almost as secure as a digital signature.

## III. Proposed Algorithm

Here, the aim is to code the facial image by extracting the feature data from the 68 landmark points landmark plotting on the face and construct a unique digital signature for an individual. With the increased number of points considered, the degree of consistency and individuality along with promptness increases. One can have data without information but it is quite impossible to have information without data. Hence it strengthens the security aspect to greater extent. Following the landmark points extraction it prepares the signature to store in the database reducing the database overhead (instead of storing the entire image file we are storing specific attributes of the encrypted image in textual format). The digital signature entirely consists of characters. There are certain constraints which must be taken care of, while plotting the landmarks. The proposed algorithm consists of three step identity evaluation technique to incorporate with these. The algorithmic steps consist of the following steps:

### *A. Smile Elimination*

When a person smiles, the orientation of the face changes and the facial landmarks are no more fixed as shown in Fig. 2. As the constancy gets disrupted, this makes it difficult for the computer to identify a face uniquely (assuming the database has stored the features of a non-smiling face of a person). Hence ambiguity occurs. It may not recognize individuals with their corresponding digital signature. Such interruptions and misinterpretations are strictly avoidable due to security concerns, otherwise the implication becomes useless.

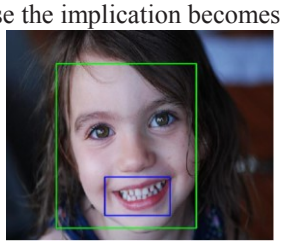

Fig. 2. Smile Detected

This makes the detection and elimination of the smile a necessary task before extracting the facial features to maintain constancy of the landmarks and mapping the data set accordingly, so that the integrity and performance of the algorithm touches required standards. This algorithm trains to computer to strictly reject the facial gesture containing smiles. In such a case the computer prompts the man to retake the picture until proper gesture can be found [10]. It acts robust to noisy training data and enables us to deal with large amount of dataset while training the computer. Hence the concern of performance efficiency gets sorted.

The proposed algorithm extracts the features based on 68 point landmark detection (as shown in Fig. 3), expected to have an accuracy of 93.88 percent. Further eliminating the smile ensured that we get a larger number of landmark points to extract the features, For example, the 2 points at the corner of the lips, eyebrows which were not static in gestures like smiling etc, but can be taken into account after smile elimination which will be quite helpful in enhancing the individuality of an individual. This leads to greater accuracy of facial recognition and more efficient extraction and analyzing strength of the facial attributes of an individual to meet the security goals. More is the number of extracting features more is the robustness of the concerning algorithm.

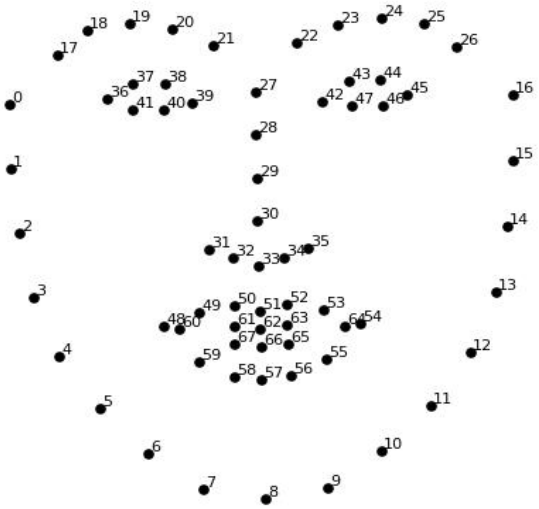

Fig. 3. Plotting of 68 Point Facial Landmarks

## B. Feature Extraction

After eliminating the smile barrier the algorithm moves forward to the feature extraction. In the study, BioID [4, 9] database of face is used [7] as shown in Fig. 4. It uses 68 point facial landmark technique mapping on individual's face to resolve identification issues. Using 68 points into consideration the recognition rate can be enhanced up to 93.88 percent. As quite a large number of points are taken into account, the feature can be analyzed with utmost perfection and clarity which enhances the security empowerment[10].

*1) CDNU Algorithm:* Next we intend to draw triangles upon the relatively fixed points among those 68 points. In this algorithm the triad combination of fixed points that has been utilized are as follows:

[57, 46, 9], [18, 27, 9], [40, 43, 34], [51, 53, 58], [32, 36, 52], [51, 53, 9], [32, 28, 36]

Fig. 4. Image Samples from BioID [9]

After that the perpendicular distance from the top most point to its opposite vertex along with the angular measurements of any two distinct angles are being obtained in order to resolve ambiguity among individuals more specifically. This method is referred as CDNU method throughout this paper, named after the initials of the names of the developers of this algorithm. The output of CDNU is shown in Fig. 5.

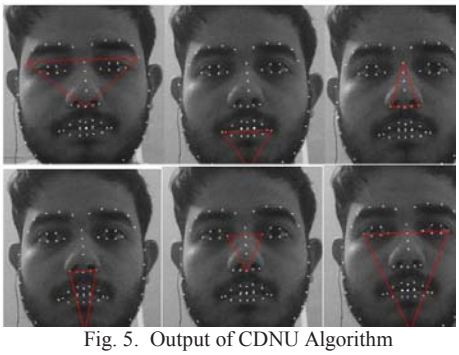

Fig. 5. Output of CDNU Algorithm

## C. Digital Signature

Once we are done with the smile elimination and feature detection the next challenge comes out to be the generation of the digital signature to identify individuals individually. The three data values taken from each triangle (perpendicular from top point to the opposite vertex, and the two opposite angular measures) out of six different triangles leads to the production of 18 (six triangles , three for each of them) different data points for a particular face. This was found to be unique for every face.

Our aim is to create a pattern (digital signature) from these data sets which will be unique for each and every individual face thus providing prominent security. From the high accuracy that we get in recognizing a face from the CDNU method, it is assured that a 36 (18 x 2) digits sequence generated in a predefined order will be unique for every face. But storage of the 36 digits will take up major amount of space. To optimize that, Huffman Coding Algorithm (as shown in Fig. 6) is implemented. It is a lossless data compression technique which will not only reduce the data size but also create a pattern that is unique to every face.

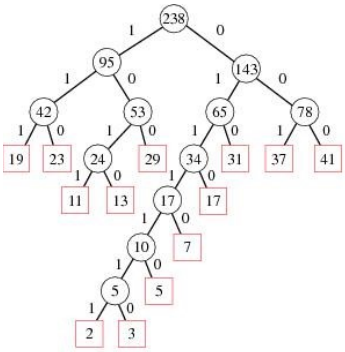


Fig. 6. Huffman Coding Application

The security aspect of the idea is also met as the encrypted code will not be easy to decode without the Prefix codes generated during encryption. The storage overhead gets reduced to a further as the entire digital signature that is the actual identity of an individual gets stored in the form of binary bits, occupying the minimal space.

As the data is stored optimistically, it enhances the ease of searching and sorting making it more compatible and desirable to the real world operating systems. The overall process is shown in Fig. 7.

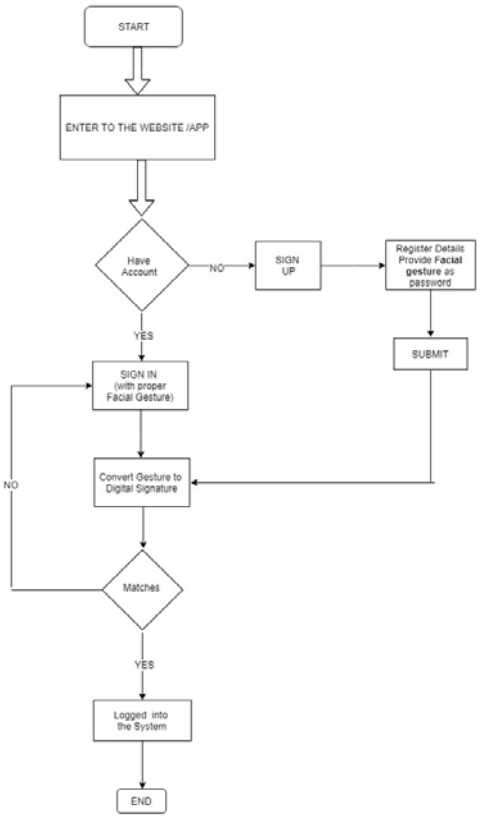


Fig. 7. Implementation Flowchart

## IV. Result Analysis

The very first step of the process is to take care that the frame is empty (shown in Fig. 8) or there are not multiple faces in the frame (shown in Fig. 9). If there are multiple faces or no face in the frame the process will immediately stop or raise an alert.

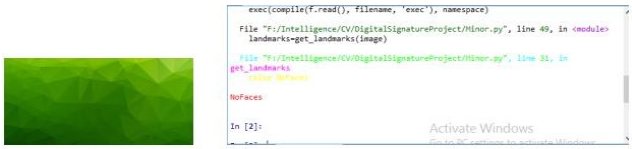


Fig. 8. Frame with No Face

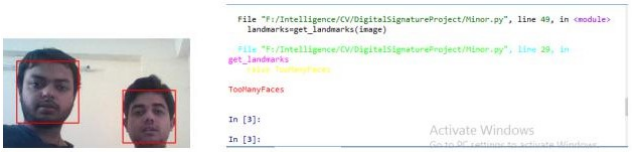


Fig. 9. Frame with Multiple Faces

When it is ensured that there is single frontal face in the frame, there shall be detection of smile. If smile is detected (shown in Fig. 10), then it would raise an alert and wait till no smile is detected before taking the snapshots.


Fig. 10. Smile Detection

Once the above mentioned problems are eliminated a certain number of snapshots of the frontal face present in the frame will be taken as shown in Fig. 11. After taking the snapshots, 68 points facial landmarks are extracted from each of those snapshots as shown in Fig. 12.

Fig. 11. Sample of Frames

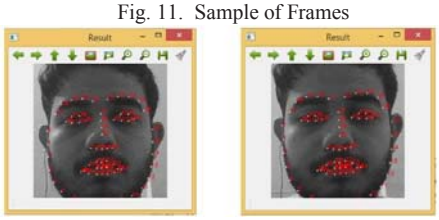


Fig. 12. Facial Landmarks with 68 points

In the individual snapshots the fixed features are marked out. For a single snapshot we shall consider three fixed features and form a triangle joining them (shown in Fig. 13). The properties of the triangle shall be unique for each face. Here we shall be dealing with the two base angles and the height of the triangle from where we shall form the digital signature.

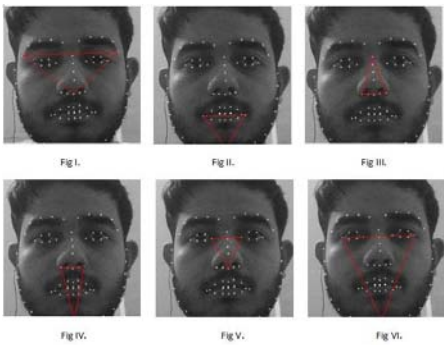


Fig. 13. Faces with Three Fixed Features

Table. I shows the base angle and the height of the triangle of these features.

TABLE I
BASE ANGLE & HEIGHT OF TRIANGLE

| Figure | Base Angle (A) (in degree) | Base Angle (B) (in degree) | Height of Triangle |
|---|---|---|---|
| 13.I | 40.85565361315895 | 39.39080460741436 | 66.65613384458226 |
| 13.II | 58.4571724872097 | 55.47976635457555 | 53.07915647451615 |
| 13.III | 72.7586276042952 | 70.88510711552262 | 58.02495176753109 |
| 13.IV | 76.87567209370903 | 78.94476881143214 | 89.03466330996166 |
| 13.V | 64.30277103517057 | 63.45610359357813 | 50.06035857881464 |
| 13.VI | 66.74627129357516 | 66.99688371693613 | 139.6079140315061 |

Input string to the Huffman compression is:

40.8556536131589539.3908046074143666.6561338445822658.457172487209755.4797663545755553.0791564745161572.758627604295270.8851071155226258.0249517675310976.8756720937090378.9447688114321489.0346633099616664.3027710351705763.4561035935781350.0603585788146466.7462712935751666.99688371693613139.6079140315061

Fig. 14 is the resultant Huffman tree storing features of an entire face.

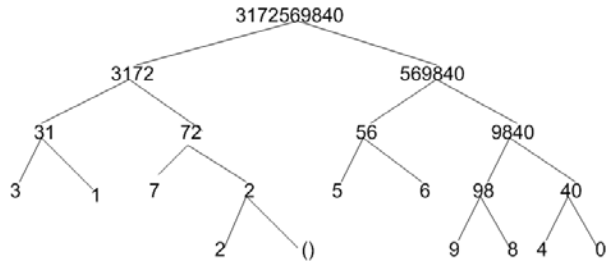


Fig. 14. Huffman Compression

In this work facial recognition was performed with the help of facial landmarks. 68 point facial landmark detection was performed on 1513 images from the BioID data. With smile detection and elimination at beginning itself, the number of fixed point's increase which further helped in strengthening the security rigidity. The co-interior angles and perpendicular height of the triangulated landmarks is used as feature data using CDNU algorithm. Next the extracted features are being used to construct the digital signature which lightens the database overhead, enhancing the efficiency of search and manipulation in a befitting manner.

## V. CONCLUSION

The result shows that landmarks are used for the facial detection and it reduces the computer overhead and enhances the performance speed and efficiency. The approach is to store just the digital signature generated in terms of binary digits into the database irrespective of the traditional systems where the entire image and related data gets stored making it too messy and expensive to deal with. Each time the user desire to signing in to the system, he/she will be directed to turn on the camera, fit his front-face within the view-port range and provide proper gesture (excluding smile and other that interrupts the constancy of the landmarks). Next once the system accepts the gesture being posed in front, the proposed algorithm converts that to the digital signature consisting of binary bits and tries to match that with the existing signatures in its concerned database. If matches are found the user is all set to proceed to the interface, if not it will redirect to the sign in Page. Similarly in case of Sign-up or Registration procedure the entire first half of the procedure will get followed, but instead of searching in the database it will store that into the database, so that can be referred in future while signing in. Thus this algorithm will remove the existence of fake accounts and anonymous identities. Individuals will be restricted to their account constraints, which will be quite helpful incorporating with the privacy of individual data and security concerns. The algorithm can further be implemented using 78 point facial landmark detection. The inclusion of greater number of points will enhance the degree of the facial feature analysis and hence improving the security standards and privacy.

## REFERENCES


[1] B.J. Saha, C. Pradhan, K.K. Kabi, A.K. Bisoi, "Robust Watermarking Technique using Arnold's Transformation and RSA in Discrete Wavelets", IEEE International Conference on Information Systems and Computer Networks, Mathura, India, 2014, pp. 83-87.

[2] N. Erdogmus, S. Marcel, "Spoofing in 2D Face Recognition with 3D Masks and Anti-Spoofing with Kinect", IEEE International Conference on Biometrics: Theory, Applications and Systems, Arlington, VA, USA, 2013, pp. 1-6.

[3] N. Nandy, D. Banerjee, C. Pradhan, "Color Image Encryption using DNA based Cryptography", Springer International Journal of Information Technology, 2018, pp. 1-8.

[4] Anil J, L. Padma Suresh, "Literature Survey on Face and Face Expression Recognition", IEEE International Conference on Circuit, Power and Computing Technologies, Nagercoil, India, 2016, pp. 1-6..

[5] T. Ozseven, M. Dugenci, "Face Recognition by Distance and Slope between Facial Landmarks", IEEE International Artificial Intelligence and Data Processing Symposium, Malatya, Turkey, 2017, pp. 1-4.

[6] S. Anishchenko, V. Osinov, D. Shaposhnikov, L. Podlachikova, R. Comley, X. W. Gao, "Toward a Robust System to Monitor Head Motions during PET based on Facial Landmark Detection: A New Approach", IEEE International Symposium on Computer-Based Medical Systems, Jyvaskyla, Finland, 2008, pp. 50-52.

[7] A. Liang, W. Liu, L. Li, M. R. Farid, V. Le, "Accurate Facial Landmarks Detection for Frontal Faces with Extended Tree-Structured Models", IEEE International Conference on Pattern Recognition, 2014, pp. 538-543.

[8] W. J. Baddar, J. Son, D. H. Kim, S. T. Kim, Y. M. Ro, "A Deep Facial Landmarks Detection with Facial Contour and Facial Components Constraint", IEEE International Conference on Image Processing, Phoenix, AZ, USA, 2016, pp. 3209-3213.

[9] BioIDFace Database, https://www.bioid.com/About/BioIDFace-Database. [Accessed: 27-NOV-2018]

[10] T. George, S. P. Potty, S. Jose, "Smile Detection from Still Images using KNN Algorithm", IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies, Kanyakumari, India, 2014, pp. 461-465.