IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Forensic Desk- Face Sketch and Recognition

[1]Prakhyath, [2]Abhijna P Naik, [3]Sudarshan Udupa, [4]Shraddha H S,
[1]Student, [2]Student, [3]Student, [4]Student
[1]Information Science and Engineering
[1]A.J. Institute of Engineering and Technolgy, Mangalore, India

Dr. Suresha D
(Project Guide)
Professor and Head, Department of Information Science and Engineering,
A J Institute of Engineering and Technology, Mangalore, India
Email: suresha@ajiet.edu.in

Abstract : In the emerging world the crime rate is increasing day-by-day,to reduce the crime rate and bring justice, we present a application which is usefull of the forensic sector for the betterment of the future.This is a standalone application, allowing user to construct accurate composite face sketch using the predefined facial feature sets provided as tools that can beresize and repositioned as per requirement/described by the eye-witness. Moreover, the constructed composite face sketch can then be matched with the law enforcement departments database using deep learning and the speed and efficiency of cloud infrastructure to identify and verify the criminal. The same process can even be done with the hand-drawn sketch making the application backward compatible with traditional approaches.In this application we are using drag and drop methods which is much easier to access and which also provides better result comparedto other traditional approach.The face recognition can be done quickly which helps the forensic department to proceed further investigations.We are developing an application which is more accurate and user friendly for the department in many aspects.

IndexTerms **– Face Recognition, Crime Rate, Sketch.**

I. INTRODUCTION

Face sketches created based on eyewitness descriptions can be used to quickly identify criminals and prosecute them. However, in today's technologically advanced society, hand-drawn sketches that are used to match and identify from pre-existing databases or real-time databases are not found to be as efficient or time-saving. In the past, a number of methods to transform hand-drawn face drawings and use them to automatically identify and recognise the suspect from the police database were offered, but these methods could not deliver the precise outcomes that were required. Applications to make composite face sketches were also introduced, but they too had a number of restrictions, such as a small selection of facial traits and a cartoonish appearance to the formed suspect. The aforementioned applications and needs inspired us to consider developing an application that would allow users to upload hand-drawn individual features on the platform, which would then be converted into the applications component set, in addition to providing a set of individual features like eyes, ears, mouth, etc. to be selected to create a face sketch. The produced sketch would therefore resemble the hand-drawn sketch much better, making it much simpler for the law enforcement agencies to modify the programme. The law enforcement team could even submit an earlier hand-drawn sketch using our app in order to use the platform's platform to identify and recognise the suspect utilising the much more effective deep learning algorithm and cloud computing.

II. PROBLEM STATEMENT

The total crime rate is rising in this day and age, and in order to keep up, law enforcement agencies must develop ways to streamline investigations and make it easier for them to convict offenders. One such method is to identify and confirm the culprit using face recognition technology.The conventional method in this case is to utilise the hand-drawn face sketches created by the forensic sketch artist to identify the offender; modernising this would entail using the hand-drawn sketch and comparing them with the database of the law enforcement agency to identify the criminal. This method would have a number of technological restrictions and take a lot of time because there aren't many forensic sketch artists accessible at the time, there are so few forensic sketch artists accessible, using this

method would result in a number of limitations with current technologies and even take a lot of time.Thus, there is a need for creating an application which would not just provide a set of individual features like eyes.

III. OBJECTIVE

- To provide a rich platform for the Forensic sector based on face construction and recognition.
- To improve the Forensic technology for faster processing.
- To implement a drag and drop function for facial elements which will be used as a sketching tools.
- In the recent studies crime rates are increasing day-by-day, the application is developed to decrease percentage of crime rate.

IV. OUTCOMES

The The applications has two main outcomes Face Construction Face RecognitionThe application provides a drag and drop function where all the face structures and elements can be draged and dropped according to the users or artists perspective.The application contains facial datsets consisting of facial parts which are used as tools for designing the sketch.Using Face Recognition it identifies the criminal sketch with the criminal database and provides the accuracy of the sketch compared with the database.Face Recognition provides a image which is compared with a sketch and provides a matched image of the criminal from the database.

V. LITERATURE SURVEY

In "Face Photo Recognition Using Sketch Image for Security System," A.Sivasangari, S.Poonguzhali, Immanuel Rajkumar, Maheshwari, et al. [1] published their research. The proposed engineering includes a large convolutional neural network (DCNN), on which exchange learning is connected using pictures and sketches1 to help the system become accustomed to the relationship between the two modalities. The decision to use an existing system rather than creating a new one is based on the author's belief that the former strategy will promote quicker mingling, relieve local minima, and foster better speculation. The benefits of DCNN [9] are as follows: 1) it was also designed to recognise faces, but only in photos; and 2) it is one of the primary FRSs for unrestricted face recognition. The input is received as an image, and if video is received, it is afterwards divided into the various video-image frames. As a result, a Login HTML page for uploading videos and turning them into images has been developed. For output, the login information is collected from the Microsoft SQL database engine. As a result, a video upload page, a video parser page, and a login HTML page have all been developed. The login information is stored in the Microsoft SQL database engine. Insert values into the table once it has been created. once the link has beenmade. The software returns while it's executing. It needs to be accessed in a browser after a video has been uploaded and scanned to get the photos scanned.

"Forensic Sketch-to-Face Image Transformation Using CycleGAN," by Nischal Tonthanahal, Sourab B R, Dr. Sharon Christa, et al. [2] A person's face sketch is processed as part of the proposed system, Forensic sketch to face transformation, to provide a realistic representation of the subject's face. An illustration of an image-to-image transformation is this. Whether it be forensic or creative, this method has a wide range of uses. It can be used in a forensic application to more clearly depict the face of a missing person or criminal using sketches created by forensic artists.When utilising conventional image processing techniques, it can be difficult to change an image from one style and texture to another. However, by learning the mappings between two high-level domains, it can be accomplished through Adversarial Style Transfer. Image generation can be done with GANs (Generative Adversarial Networks). In order to implement this, CycleGAN is employed. Generative Adversarial Networks is a subset of it. It functions without needing samples of source and destination photos in pairs. The availability of training samples with the same subject in both domains is a need for techniques like Pix2PixGAN [1].

An FPGA-Implemented Parallel System of Face Recognition, for Digital Forensics Applications by Maria Pantopoulou Nicolas Sklavos et al. The suggested system was created in VHDL, and Xilinx's Vivado Design Suite et.al[3] was used to synthesise and implement it. For a Xilinx Artix-7 FPGA, the Local Binary Patterns Histograms method was implemented (xc7a75tcsg324-3). The 165 photos from the Yale face database were utilised to assess the system's accuracy, and the results of the experiment are shown in Table I. The system's overall execution time, which includes the time required to compute the characteristic vectors of each image and the time required for each recognition, is close to 128 milliseconds. This is due to the large number of photographs in the database that is being used and the utilisation of the online training procedure. Additionally, the pixels of the images and the test image's characteristic vector are stored in the BRAMs that were allotted. Finally, employing a database of 165 320x243 grayscale photos representing fifteen persons, the system's best accuracy was equal to 80% for 30 consecutive trials. It is displayed how the quantity of photographs in the database and the recognition time correlate.

"Towards facial recognition using likelihood ratio approach to facial landmark indices from photos," by Rajesh Verma, Keval Krishna, et al.[4] The project suggests a cutting-edge method for facial comparison in a forensic setting. We used an automated method to identify facial landmarks, and from a subset of these landmarks, we generated independent facial indices. Due to posture changes, it is challenging to compare the morphometric indices, hence a statistically sound method is needed for face comparison. An automated method was used to identify facial landmarks, and from a subset of these landmarks, independent facial indices were chosen. Due to posture changes, it is challenging to compare the morphometric indices, hence a statistically sound method is needed for face comparison.In a database of 40 people, with 10 facial photographs of each, in various poses,

expressions, lighting, and backgrounds, the current work displays the application of likelihood ratios (LRS) to evaluate the grouping of facial images based on the morphometric indices. A true positive (TP) rate of 85% and a false positive (FP) rate of 25% were obtained using the criterion LR 1 for proper categorization and only taking into account indices that are not correlated. The team also determined the performance measures for evaluating the validity and dependability of the likelihood ratio technique, and they discovered that the log likelihood ratio cost was 0.26.

In "On Designing a Forensic Toolkit for Rapid Detection of Factors that Impact Face Recognition Performance When Processing Large Scale Face Datasets," by J. Rose and T. Bourlai et al. [5], There have been a number of intriguing applications that bridge the gap between the two sciences and improve connections between the connected groups because of the overlap between the domains of forensic investigation and biometric recognition, including face recognition. The purpose of these applications is to provide computer assisted and biometric capabilities to law enforcement personnel. As a result, using biometric algorithms to forensics can aid law enforcement inquiries in a variety of contexts. even locate people of interest using soft biometrics like scars, markings, and fingerprint comparisons, sketch-to-photo face comparisons.In this book chapter, the project is focused on facial recognition, which can be used to help provide clues when other forensic evidence is unavailable or not present. Most importantly, facial recognition can help investigators avoid the time-consuming process of manually interviewing potential witnesses. The operators will be able to examine enhanced group, or exclude face data before processing thanks to the proposed forensic toolkit.

Face recognition is one of the most actively researched areas of computer vision and pattern recognition, with many practical and commercial applications including identification, access control, forensics, and human-computer interactions, according to Insaf Adjabi, Abdeldjalil Ouahabi, Amir Benzaoui, and others [6]. Finding a face in a crowd brings ethical problems and major concerns about personal freedom. To research constrained and unconstrained face recognition, a select few major methodologies, algorithms, approaches, and databases have been suggested in recent years. A certain level of maturity and extremely high rates of recognition were recorded for 2D techniques. Additionally, the performance is obtained in controlled settings with predetermined acquisition characteristics, such as lighting. As an alternative to the issues outlined above, 3D methods were suggested. The benefit of 3D data is that it is independent of position and lighting conditions, which has increased the effectiveness of recognition algorithms. However, the sensitivity of 3D data to changes in facial expressions is limited. The development of facial recognition technology over time, cutting-edge methods already in use, and potential directions are all covered in this review. They have focused primarily on the newest databases and 2D and 3D face recognition techniques. Additionally, they paid special attention to the deep learning approach because it reflects the reality in this area. In order to give the reader a point of reference for themes that need investigation, open concerns are reviewed and potential routes for facial recognition research are suggested.

Deisy Chaves, Eduardo Fidalgo, Enrique Alegre, Rocio Alaiz-Rodrguez, Francisco Jáez-Martino, and George Azzopardi et al. [7] published a study titled "Assessment and Estimation of Face Detection Performance Based on Deep Learning for Forensic Applications" in which they found that face recognition is a useful forensic tool for criminal investigators because it However, because it must be able to work with low-quality photographs of real-world environments and meet time-sensitive demands, it is a very difficult assignment. Although deep learning methods for face detection have shown to be quite effective, they demand a lot of processing time and power. On the WIDER Face and UFDD data sets, they investigated the speed-accuracy trade-off of three widely used deep-learning-based face detectors using a variety of CPUs and GPUs. They have also created a regression model that can predict performance in terms of speed and precision. Then, they anticipated that it would develop into a very helpful tool for the end user in forensic laboratories to gauge the effectiveness of various face detection approaches. According to experimental findings, resizing images in CPUs and GPUs to 25% and 50% of their original sizes, respectively, yields the optimum speed-accuracy tradeoffs. Multiple linear regression models with a mean absolute error (MAE) of 0.113 were used to estimate the performance of Atlast.

The authors of "Component-based face recognition under transfer learning for forensic applications," Rupali Sandip Kute, Alwin Anuse, Vibha Vyas, et al. [8], note that in many forensic application scenarios, only a partial face image is provided for recognition. As a result, systems that work with partial face images and face component images have become extremely important. This study outlines a unique method for component-based face identification and association under transfer learning and shows how the information learned from entire face images can be used to categorise face components. Ears, mouth, and nose—three crucial facial features—are employed for association and identification. These elements are particular, consistent, and unaffected by variations in poses and facial expressions. The face and lips, the face and ears, and the face and nose are all associated. Despite coming from various domains, these face components and the face itself communicate information that is used to transmit knowledge from one domain to another. For the correlation between complete and partial face images, various half-face kinds are taken into account, including left, right, upper, and lower half as well as left, right, upper, and lower diagonal. The suggested method can be used for holistic face recognition, component-based face identification, and partial face recognition due to the association between a face and its many components.

According to Zhaoguang Pan, Yanli Ren, and Xinpeng Zhang et al. [9] in "Low-complexity fake face detection based on forensic similarity," face synthesis and manipulation technology have advanced quickly in recent years, making it possible to create incredibly lifelike fake face videos that are capable of fooling face recognition systems that are already in use. Allowing phoney face videos to circulate on the Internet could lead to major ethical, moral, and legal issues due to the excellent quality of fake footage. To tell phoney face recordings apart, an efficient and trustworthy detection approach is urgently needed. They have observed that most face forging techniques currently in use extract the face portion of each frame first and then only alter the

face portion of each frame, leaving the background intact. As a result, in a forged face frame, the disparity between the face area and the background area is substantially greater than the difference in the identical unforged frame. The forensic similarity method, which evaluates the authenticity of face video frames by identifying the difference in similarity between the face area and the background area, is a new detection technique introduced in this study based on such observation. The generalisation capacity on the Celeb-DF dataset was assessed after training and testing on the FaceForensics++ dataset for evaluation. According to the experimental data, the proposed technique performs better or equally well, particularly in terms of generalisation ability. Under the Celeb-DF dataset, our model can achieve 8–12% accuracy increases over Xception.

A Forensic Method for DeepFake Image based on Face Recognition by Jian Wu, Kai Feng, Xu Chang, Tongfeng Yang et al [10]. Digital photographs that are DeepFake have a detrimental effect on social security, legal forensics, and news accuracy. A face recognition-based technique is suggested in order to more reliably identify DeepFake digital photos. Facenet extracts the feature vectors from the face images, and as a classification rule, it calculates the Euclidean distances between the feature vectors of various face images. Then, real and false face photos are binary classified using machine learning techniques. The suggested method has a superior detection effect than the current detection methods, according to the experimental findings on the Celeb-DF data set.When two fields collide: Identifying super-recognizers for neuropsychological and forensic face recognition research, Sarah Bate, Emma Portch, Natalie Mestry, et al. [11] write that while the field has long been interested in people's inability to recognise their own faces, it has more recently become interested in the ability to recognise facial identity.It is evident that the average population's facial recognition abilities vary greatly. Those allegedly living at the extreme top of this spectrum are referred to as "superrecognisers." On the one hand, cognitive neuropsychologists who are eager to learn more about these individuals are of interest to them.Researchers in the forensic face matching field assess the use of super recognisers in actual police and security contexts, while researchers from the face recognition continuum field assess the commonality of the face recognition continuum. There are differences in the definition as a result of these two distinctly different methods.a lack of consistency that prevents theoretical advancement in the study of super-recognisers and, maybe more fundamentally, the method used to detect them here, we evaluate the techniques utilised in published research to identify super-recognisers and offer a universal definition and screening guidelines that may be followed in all disciplines.

Maelig Jacquet et al. [12] have suggested a review of the literature leading to the establishment of a methodological workflow to develop a score-based likelihood-ratio computation model using a Bayesian framework. Their article is titled "Automated face recognition in forensic science: Review and perspectives."Regarding the modelling of within-source and between-source variability distributions, various strategies are put out in the literature. The modelling technique might be either case-specific or generic, depending on the data that are available.Without any photographs of the suspect at hand, generic procedures enable interpretation of the score. As a result of the data not being tied to the suspect, such a model is much more difficult to defend in court.The discriminating power and the calibration state of the model should be used to evaluate the performance of the model in order to ensure that the generated score-based LR is robust. Consequently, define the primary measurements and graphical depictions used to express the performance attributes in numerical and visual form.

Little is known about how effectively human operators can use these AFRS as decision-aids, as demonstrated by Carragher, D. J., Hancock, P. J. B. et al. [13] in "Simulated Automated Facial Recognition Systems as Decision-Aides in Forensic Face Matching Tasks" in which they compared the performance of AFRS and humans on tasks of one-to-one face matching.The goal was to determine how a prior AFRS choice impacts human performance on a face matching task and whether human oversight of AFRS decisions can improve the human-algorithm team's performance collectively.A actual, cutting-edge Deep Convolutional Neural Network (DCNN) AFRS's performance on the identical test was used to guide the identification decisions made by the simulated AFRS.Over the course of five pre-registered tests, human operators improved their own face matching ability compared to baseline by using the judgements from highly accurate AFRS (> 90%) (sensitivity gain: Cohen's d = 0.71-1.28; total accuracy gain: d = 0.73-1.46).Nevertheless, despite this advancement, AFRS-assisted human performance continually fell short of what the AFRS was able to accomplish on its own. Participants said that even when the AFRS only made mistakes on face combinations with the highest human accuracy (> 89%),questions were raised regarding the circumstances in which human monitoring might improve AFRS operation because it frequently failed to fix the system's mistakes while also overturning many good ones.Overall, these data show that this straightforward model of human-AFRS teaming has limitations due to the human operator. The "human-in-the-loop" approach to AFRS monitoring in forensic face matching scenarios is affected by these findings.

In "A Review of Face Analysis Techniques for Conventional and Forensic Applications," by H.T. Chethana, T.C. Nagavi, et al. [14], forensic specialists utilise manual comparison and domain-specific techniques to identify the suspects.It takes longer and requires more work to compare manually. As a result, creative solutions to automate the use of domain-specific procedures can be created.This chapter's major goal is to explain why face recognition is a crucial and crucial topic in forensics and what obstacles there are in forensic face recognition. Given that forensic facial recognition research is still in its infancy, these researchers will be encouraged to pursue it.

The development of biometrics for human identification is described in "New Solutions for Automated Image Recognition and Identification: Challenges to Radiologic Technology and Forensic Pathology" by Jungi Morishita, Yasuyuki Ueda, et al. [15].In "New Solutions for Automated Image Recognition and Identification: Challenges to Radiologic Technology and Forensic Pathology," by Jungi Morishita, Yasuyuki Ueda, et al. [15], the authors discuss patient verification during medical imaging procedures like computed tomography and magnetic resonance imaging as well as the development of the first biological fingerprint techniques for digital chest radiography.Automated image recognition and identification systems created for clinical

photos without metadata may also be used to identify unidentified people or victims of large-scale disasters.Radiologic technology, patient safety, forensic pathology, and forensic odontology are still in the early phases of developing techniques that are adaptable to a wide range of contemporary imaging modalities. Its significance in actual practise will, however, keep growing.

In this study, we give a thorough and critical analysis of face identification methods, following the suggestion made by Erik Hjelms, Boon kee low, et al. [16] on the topic of "Face Detection using Computer Vision and Image Understanding" survey. In order to locate and separate the face region from the backdrop, face detection is a crucial first step in face recognition systems. Additionally, it has a number of uses in fields like intelligent human-computer interfaces, video coding, video conferencing, crowd monitoring, and content-based picture retrieval. The face detection issue, however, did not garner much attention from academicsuntil lately. Face detection is a challenging topic in computer vision because the human face is a dynamic object with a great degree of diversity in its appearance. There have been many different ways put forth, from straightforward edge-based algorithms to composite high-level systems leveraging cutting-edge pattern recognition techniques. The algorithms covered in this study are categorised as either feature-based or image-based, and their technical approach and effectiveness are reviewed. We do not offer a thorough comparative evaluation due to the lack of standardised testing, however comparisons are provided when findings are reported on widely used datasets. We also show some suggested applications and potential application domains.

"Accuracy Comparison Across Face Recognition Algorithms" was a topic suggested by Jacqueline G. Cavazos, P. Jonathan Philips, and others [17]. How Accurate Are Older Face Recognition Algorithms for Images of Different Races, and Where Are We on Measuring Race Bias? (race bias). Here, we discuss methodological issues for evaluating racial prejudice in algorithms as well as potential underlying reasons (data-driven and scenario modelling). We examine both data-driven aspects that take into account the "user" of the algorithm (e.g., image quality, image population statistics, and algorithm architecture) and scenario modelling factors (e.g., threshold decisions and demographic constraints). We present data from four facial recognition algorithms (a previous-generation algorithm and three deep convolutional neural networks, DCNNs) for East Asian and Caucasian faces to demonstrate how these difficulties are relevant.

Joint face detection and Facial Landmark Localization FLL utilising graph match and pseudo label was suggested by Zhiqun Pan, Sunije Zhang, et al. [18]. Because training samples with annotations of both facial landmarks and bounding boxes are expensive to obtain, author linkages open overlay panel with FLL are not integrated well. In this paper, a real-time framework for FLL and collaborative face detection is presented. In order to predict the locations of facial landmarks and face regions, we first take advantage of the overlap between the two tasks and create a fully convolutional network. In addition, we recognise the cluster assumption in FLL and suggest a gradually pseudo labelling training that not only gets rid of the negative effects of inaccurate or noisy annotations, but also fully utilises exact, inexact, and coarse-grained labels.

Researchers recently discovered that the intended generalizability of (deep) face recognition systems enhances their vulnerability to assaults, as highlighted by Ulrich Scherhag, Christian Rathegeb, Jonathan Merkle et al. [19] in their paper "Face Recognition Systems Under Morphing Attacks." Particularly, face recognition systems are seriously at danger from assaults based on modified face photos. A number of biometrics research laboratories have recently become interested in the problem of (facial) image morphing and automated morphing attack detection, and numerous methods have been published as a result. This research presents a conceptual categorization, criteria for evaluating such strategies, and a thorough literature review of pertinent works. Additionally, the surveyed methodologies' technical considerations and tradeoffs are discussed along with open issues and challenges in the field.

The topic of "Forensic face recognition based on KDE and evidence theory with Forensic face recognition (FFR)" has been explored in recent years in forensic science, according to Wen Xiao1 et al. [20]. The output scores of an automatic face recognition system are used to represent how similar two face image pairings are, but they are not appropriate for forensics. In this paper, a score-mapping model based on evidence theory and kernel density estimation (KDE) is developed. For each dimensional feature vector of the face picture pairs, the probability density function (PDF) was first generated using KDE. The basic probability assignment (BPA) of supporting the prosecution hypothesis and the defence hypothesis might then be determined separately using the PDFs. To obtain the final BPA, which measures the strength of evidence support, Dempster's rule was used to aggregate the BPAs of each characteristic. The experimental findings show that the suggested method outperforms the traditional KDE-based likelihood ratio method in terms of accuracy, sensitivity, and specificity.
used in laboratories etc.

VI. REQUIREMENT SPECIFICATION

- **Security and Privacy**
  The major concern of the law enforcement department before adapting any system is security and privacy. Keeping this in mind the application is designed to protect the privacy and carry out the security measures in the following ways.
- **Machine Locking**
  The Machine locking technique would ensure that the application once installed on a system could not be tampered and could not been operated on any other system, for which the application uses two locking parameters i.e. one software and one hardware locking parameter.

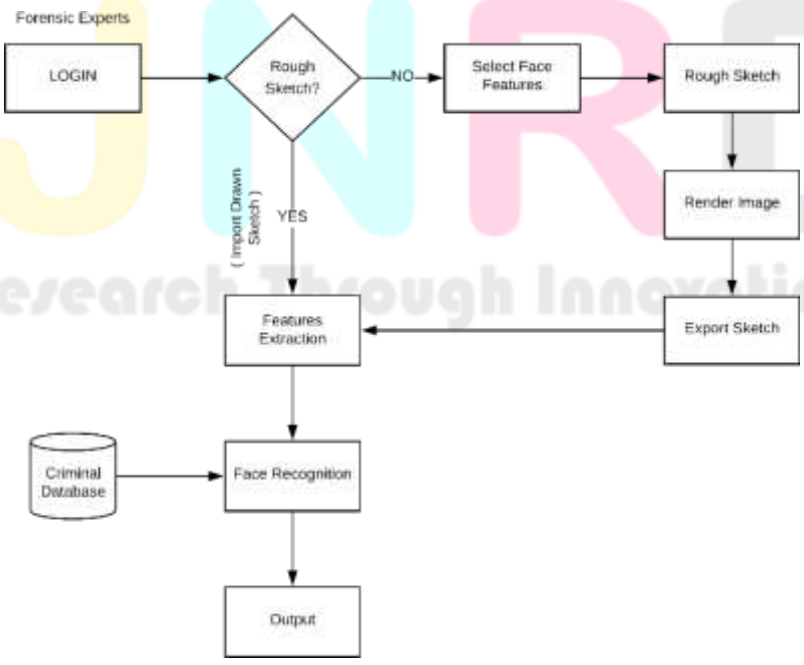
- **Two Step Verification**
  Every law enforcement authorized user would be given an official E-Mail ID which would use to login on to the application, thus using this step would require the user to enter a random code been shared with them on their mobile/desktop in order to complete the logging process.
- **Centralized Usage**
  The system which has the application been installed would be connected to a centralized server of the law enforcement department campus containing the database and the other important feature set of the application, thus the application could not be operated once disconnected from the server.
- **Backward Compatibility**
  The major drawback in adapting any new system is the complication been involved in completing migrating from the previous technique to the new technique, Hence resulting in the wastage of time resources. To overcome this issue, we have designed our application in such a way that even the hand drawn sketches can be uploaded and the user can use the deep learning algorithms and cloud infrastructure to identify and recognize the criminal using the hand-drawn sketch.

- **Hardware Requirements**
  This application is been designed to run on the minimum possible configuration of hardware.
  Processor:- Intel Core i5
  RAM: 4 GB and above
  Hard Disk: 250GB and above

- **Software Requirements**
  Client/ Node Machine:
  Operating System: Windows 7 and above
  Framework: Java JDK
  Cloud: Amazon Web Services CLI
- **Server Machine:**
  Operating System: Windows Desktop OS or Windows Server Edition
  Framework: Java JDK
  Cloud: Amazon Web Services CLI
  Database: SQLit

VII. SYSTEM DESIGN

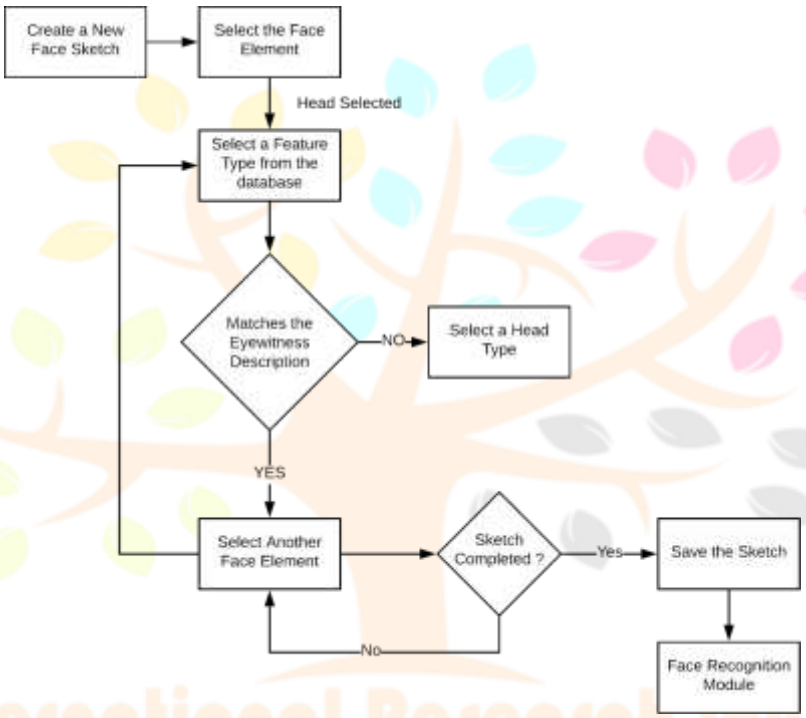
The proposed method offers a platform for forensic artists to draw in accordance with suspect descriptions using drag and drop technology, which makes it simple for the artist to draw a criminal face and cuts down on work time. It also offers a platform for face recognition technology to identify the sketch, which compares it to a criminal database and verifies its accuracy. The application would be primarily utilised by law enforcement agencies to shorten the total amount of time needed to prosecute a criminal, as well as to improve worker efficiency and speed up the system while maintaining accuracy. Because of this, the platform is made to be as basic as possible so that a user can generate a sketch in the application without receiving professional training. The architectural layout shown above depicts how the system works generally, from the login page to the results that are displayed once the sketch is compared to the database entries.



Beginning with the login page, which is divided into two pieces, privacy and security are taken into consideration right away. The login page retrieves the Mac Address, IP Address, and HDD ID in the beginning, which are then compared to the data gathered. In order to ensure that the user accessing the platform can have complete privacy and security with the data and their credentials, the second stage of the process involves authenticating the user. In order to prevent anyone other than the verified user from accessing the platform, even with the login credentials, we employ two-step verification. When the user enters their credentials on the platform, it first verifies their authenticity before sending an OTP to the registered email address.

VII. FACE SKETCH CONSTRUCTION DESIGN

As was already indicated, security and accuracy were the main characteristics on which we concentrated when designing our platform for the law enforcement division. As a result, the major goal of this project module is to create a facial sketch using the description that the Eye Witness gave to the law enforcement agency. The dashboard is designed simply to encourage no professional training to be completed before using this platform, saving time that would have required a lot of time and resources from the Department. The above illustrates the users flow being followed by the platform to provide and construct accurate face sketches based on the description.



Keeping it simple thus ensures that the user doesn't have to be a professional sketch artist from the forensic department rather any one from the law enforcement department usingthe descriptions narrated by the eye witness or in some cases the eye witness too can take controlof the platform but that would not be recommended as it can tamper the security protocols. Moving further the dashboard consists of Five main modules, First the important module is the Canvas been shown at the middle of the dashboard which would house the face sketch components and the elements of the face sketches helping in the construction of the facesketch.

Creating the face sketch would be a complicated thing if all the face elements are givenall together and in an unordered manner making the process difficult for the user and complicated to construct an accurate face which would be against the agenda aimed in the proposed system. So, to over come this issue we planned on ordering the face elements based on the face category it belongs to like head, nose, hair, eyes, etc. making it much easier for theuser to interact with the platform and construct the face sketch. This is available in the columnin the left on Canvas on the dashboard click on a face category allows user to get various otherface structure. Coming to the various face elements in a particular face category we could have multipleand n number of elements for a single category, so to solve this our platform would use machinelearning in future to predict the similar face elements or predict an suggest the elements to be selected in the face sketch but this would only work once we have appropriate data to train themodel on this algorithm and work to enhance the platform. So, now when the user clicks on a particular face category and then a new module to the right of the canvas opens and lets user to select an element from the option of face elementsto construct a face sketch. This option can be selected be selected based on the description provided by the eye witness.

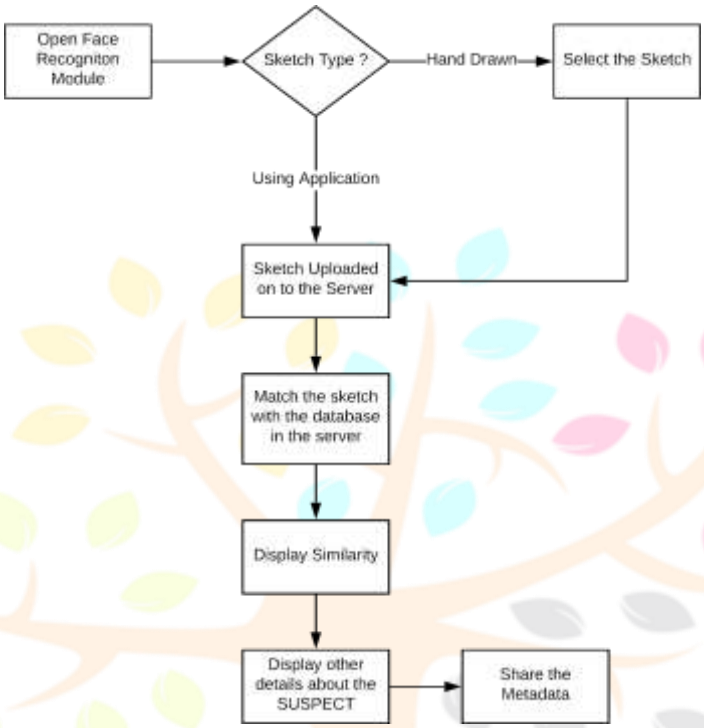
The elements when selected are shown on the canvas and can be moved and placed as per the description of the eye witness to get a better and accurate sketch and the elements havea fixed location and order to be placed on the canvas like the eye elements would be placed over the head element irrespective of the order the were selected. Same for every face element. The final module is the options to enhance the use of the dashboard, suppose in cases the user selects an element which is not to be selected so that could be rectified using the optionto erase that particular element which would be seen when selecting the face category from theleft panel.

The major important buttons are placed in the panel on the right which has a buttonto completely erase anything on the canvas of the dashboard making it totally blank. Then we have a button to save the constructed face sketch, saving the face sketch as

a PNG file for better future access. This could be any location on the host pc or on the server depending on the Law Enforcement Department.

VIII. FACE RECOGNITION DESIGN

As was already indicated, security and accuracy were the main characteristics on which we concentrated when designing our platform for the law enforcement division. As a result, the major goal of this project module is to accurately and confidently identify a face sketch in the face photo records of the Law enforcement department.



The dashboard is designed simply to encourage no professional training to be completed before using this platform, saving time that would have required a lot of time and resources from the Department. The above design illustrates the users flow being followed by the platform to provide a recognise accurate face sketch based on the description. By keeping it straightforward, it is ensured that anyone from the law enforcement branch can use the descriptions provided by the eye witness instead of requiring a professional sketch artist from the forensic department. In some cases, the eye witness may even be able to take control of the platform, though that is not advised because it could compromise the security protocol

IX. CONCLUSION

From the very first splash screen to the very last screen, the project "Forensic Desk- Face Construction and Face Recognition" is designed to keep real-world scenarios in mind as it retrieves data from the records, with security, privacy, and accuracy being the primary considerations in each scenario. When compared to previous studies in this field, the platform even contains elements that are unique and distinctive. By standing out from all other relevant research and suggested systems in this area, these features improve the platform's overall security and accuracy. Even while there is a lot of research being done on the creation of new approaches and strategies to enhance the performance of the most advanced face recognition systems now available, less effort is being made to integrate face recognition technology with the judicial and legal systems. There hasn't been anything written on how the face recognition system can be used for forensic purposes outside of a few papers.

X. REFERENCES

[1] A.Sivasangari, S.Poonguzhali, Immanuel Rajkumar, Maheshwari, "Face Photo Recognition using Sketch Image for Security System", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue- 9S2, July 2019.

[2] Maria Pantopoulou, Nicolas Sklavos, "An FPGA-Implemented Parallel System of Face Recognition, for Digital Forensic Applications", IEEE 10th International Conference on Consumer Electronics, 20466685, 10.1109/ICCE-Berlin50680.2020.9352182, 2020.

[3] Nischal Tonthanahal, Sourab B R, Dr Sharon Christa, "Forensic Sketch-to-Face Image Transformation Using CycleGAN", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 08 Issue: 07 | July 2021 www.irjet.net p-ISSN: 2395-0072, 2021.

[4] J.Rose and T. Bourlai, " On Designing a Forensic Toolkit for Rapid Detection of Factors that Impact Face Recognition Performance When Processing Large Scale Face Datasets", Part of the Adavanced Sciences and Technology for Security Applications book series (ASTSA),2020.

[5] Rajesh Verma, Navdha Bhardwaj, Arnav Bhavsar and Kewal Krishan, "Towards facial recognition using likelihood ratio approach to facial landmark indices from images", Forensic Science International:Report, volume:5, 100254,July 2022.

[6] Insaf Adjabi, Abdeldjalil Ouahabi, Amir Benzaoui and Abdelmalik Taleb-Ahmed," Past, Present, and Future of Face Recognition:A Review", Department of Computer Sciences, LIMPAF, University of Bouira, Bouira 10000, Algeria;i.adjabi@univ-bouira.dz, MDPI, 23 July 2020.

[7] Deisy Chaves , Eduardo Fidalgo , Enrique Alegre, Rocío Alaiz-Rodríguez, Francisco Jáñez- Martino and George Azzopardi, "Assessment and Estimation of Face Detection Performance Based on Deep Learning for Forensic Applications", Department of Electrical, Systems and Automation, Universidad de León, 24007 León, Spain; eduardo.fidalgo@unileon.es (E.F.); enrique.alegre@unileon.es (E.A.); rocio.alaiz@unileon.es (R.A.-R.); fjanm@unileon.es (F.J.-M.), MDPI, 11 August 2020.

[8] Rupali Sandip Kute, Vibha Vyas and Alwin Anuse, "Component-based recognition under transfer learning for forensic applications", Information Sciences volume 476, science direct, February 2019.

[9] Zhaoguang Pan, Yanli Ren and Xinpeng Zhang, "Low-complexity fake face detection based on forensic similarity", Multimedia Systems volume 27, pages353-361, SpringerLink, 2021.

[10] Jian Wu, Kai Feng, Xu Chang, Tongfeng Yang, "A Forensic Method for DeepFake Image based on Face Recognition", Association for Computing Machinery NewYork, United States, 25 August 2020.

[11] Sarah Bate , Emma Portch and Natalie Mestry, "When two fields collide: Identifying super-recognisers for neuropsychological and forensic face recognition research", Vol. 74(12) 2154–2164 Quarterly Journal of Experimental Psychology, 2021.

[12] Maëlig Jacquet,"Automated face recognition in forensic science: Review and perspectives", School of Criminal Justice, Faculty of Law, Criminal Justice and Public Administration, University of Lausanne, Switzerland, Forensic Science International Volume 307, February 2020.

[13] Carragher, D. J., & Hancock, P. J. B., "Simulated automated facial recognition systems as decision-aids in forensic face matching tasks", Journal of Experimental Psychology: General. Advance online publication. https://doi.org/10.1037/xge0001310, 2022.

[14] H T Chethana and Trisiladevi C Nagavi, "A Review of Face Analysis Techniques for Conventional and Forensic Applications", Cyber Security and Digital Forensics, 223-240, 2022.

[15] Junji Morishita and Yasuyuki Ueda, "New solutions for automated image recognition and identification: challenges to radiologic technology and forensic pathology", Radiological physics and technology 14 (2), 123-133, 2021.

[16] Erik Hjelmåsa and Boon Kee Lowb, "Face Detection: A Survey", Department of Informatics, University of Oslo, P.O. Box 1080, Blindern, Oslo, N-0316, Norway, Computer Vision and Image Understanding volume 83, 2019.

[17] Jacqueline G. Cavazos, P. Jonathon Phillips and Carlos D. Castillo, “Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?”, IEEE, 2020.

[18] Zhiqun Pan, Yongxiong Wang and Sunjie Zhang, “ Joint face detection and Facial Landmark Localization using graph match and pseudo label”, Signal Processing: Image Communication volume 102, 116587, sciencedirect, March 2022.

[19] Ulrich Scherhag, Christian Rathgeb, Johannes Merkle and Ralph Breithaupt, "Face Recognition Systems Under Morphing Attacks: A Survey", IEEE DigitalObjectIdentifier10.1109/ACCESS.2019.2899367, 2019.

[20] Wen Xiao, “Forensic face recognition based on KDE and evidence theory”, MATEC Web of Conferences 336, 06008, https://doi.org/10.1051/matecconf/202133606008, 2021.