An Improved Feature Selection-Based MSVM Classification Model for Face Presentation Attack Detection System

GAURAV SHARMA
Research Scholar, MASTER OF TECHNOLOGY in Computer Science & Engineering, Indo Global College of Engineering , Abhipur , New Chandigarh ,Punjab ,India
gauravsharma1999nov@gmail.com

VANITA RANI
Assistant Professor in Computer Science & Engineering
Head of Department , Computer Science & Engineering
Indo Global College of Engineering , Abhipur , New Chandigarh ,Punjab ,India

Abstract- In current years, with the growth of the Internet, individuals have been in the area of research, which has approved roughly a volatile increase in the capacity of evidence. People frequently practice biometrics for uniqueness validation in specific access controllers and additional features because the public's faces or thumbprints are exclusive. In this favor, FR is the crucial recognition technique with general fitness for the public's lifetime. It is mostly customs graphic imaging of social faces to observe and identify persons. Face recognition (FR) is the fundamental recognition structure that carries excessive availability to people's lives. It is commonly used for photophobic imaging of social faces to differentiate and identify personalities. In this article represent develop an improved feature selection-based multi-class (IFSBMSVM) classification (MSVM) classification model for the face PAD system. Initially, to analyze and learn various existing feature extraction and presentation attack detection techniques used for FR systems. Different types of databases such as NUAA, REPLAY ATTACK, and CASIA are used for input image data. For this purpose, the SIFT (Scale-invariant feature transforms) method extracts some valuable features from a sample. SIFT is a technique for individual and extracting built-in feature descriptors from images. Then, to project and recommend an improved feature selection-based MSVM classification model to detect the face PA images. The Grey Wolf Optimizer (GWO) method is utilized for feature selection processing. Finally, developing a face PAD system requires some performance parameters such as an accuracy (Acc) value of 95.6 % and an HTER (half total error rate) value of 3.3%.

Keywords- *Face Presentation Attack Detection System (FPAD) , Improved feature-selection based MSVM classifier, Grey wolf optimizer (GWO), Scale Invariant Feature Transformation, Half total error rate (HTER).*

I. INTRODUCTION

Over the years, FR (face recognition) has experienced important enhancements, making it one of the most widely adopted biometric modalities. Though, FR (face recognition) systems are disposed to several attacks, degrading system security, and reliability. PAs (presentation attacks) are global between these attacks. PAs are the simulated of real user faces in the form of a video, mask, and photo. Frauds attempt to avoid FRS FRSs using PA variants [1]. Utilizing these PAs, frauds can either complicate [2]. Imitation is the procedure of achieving entrance through FRSs, utilizing the imitation of real face properties. By confusing a customer’s ID, obfuscation gives them to pass a safety system disregarded. PAs have different categories such as two and three-dimensional attacks [3]. Video and photo attacks are two-dimensional attacks, whereas three-dimensional masks and makeup attacks are 3D attacks. An online entrance is attacked using simple attacks like video and photo. During border control situations, imposters utilize more refined attacks like make-up to fool safety systems [3].

PAs in the FRS happens during unauthorized access or an adversary attempts to mimic genuine persons by giving fake facial biometrical information such as common attacks such as a video, photograph, and mask. These types of attacks get illegal use of biometric verification models. Therefore, PAs in FR models are generally considered in numerous forms. The representation of different types of printed photos, and repeating a video related to a theme, are simple illustrations of 2D PAs attacks. More refined attacks include developed traditional 3-D masks that are parallel to a target-specific personality for imposture and to avoid identification. For the consistent procedure of FR technology, it is essential to progress PAD systems to identify such PAs computerized. The common field of these investigation arrangements with the recognition of print as well as replay attacks through observable spectral statistics. Maximum techniques depend on the restrictions of PAIs and performance degradation of the recalled model. Different types of features like motion, color, texture, and physical indications, are a lot of leverage for PAD in imageries from observable range. The face is measured as the utmost significant portion of the human structure. It delivers a vital role in recognizing and authenticating an individual. Because of this reason, it is also utilized in several applications in the lifecycle [4].

FPAD (face presentation attack detection) techniques developed hand-crafted properties in early analysis. These properties were categorized using ML (machine learning)[5,6,7,8] methods like SVM (support machine learning), RF (random forest), LBP (local binary pattern), HoG (histogram orientation gradient), etc. These approaches performed well in intra-database calculation with public face anti-spoofing (FAS) databases. Through, hand-crafted properties, normally texture-based features, may be particular to the situations considered within individual databases, and the ML classification methods further discussed this.

Faseela et al., 2022 [9] discussed CNN (convolutional neural network) method for classification purposes. This method comprised TL (transfer learning), AD (anomaly detection), methods, etc. Within TL, there are two added types such as domain adaptation, and domain generalization. It calculates the presentation and generalizability of models proficient on data aggregated. Pre-trained models such as Vgg-16, ResNet-50, Inception v3, and denseNet-121 were trained on the NUAA dataset. The main motive of this article is a framework that calculates how publicly available FAS databases may be combined to improve inter-database performance.

The important contributions of this research article are:

(i) To analyze and study different feature extraction methods such as LBP, HoG, SURF, GWT, etc., and presentation attack detection methods used for FRS.

(ii) To develop a feature extraction process using SIFT algorithm to extract the features in the form of KPs (key points) after that it has been implemented an improved feature selection-based MSVM (GWO and MSVM) classification model to detect PAs in the face images.

(iii) It evaluates and authorizes the face PAD system performance parameters such as Acc (accuracy), HTER, EER (equal error rate), etc., and compared with existing pre-trained TL models.

The lasting section of this research article is as surveys: The “Literature of Review” section studies existing methods and implemented techniques for face PAD systems. The database, methods, and simulations are discussed in the Material and Methods. A brief discussion of the attained outcomes is defined in the “result analysis” section. This research article is concluded in the “Conclusion” section defining further improvements.

II. LITERATURE OF REVIEW

Face PAD detection has been widely studied and applied globally for user identification. The reliability of identification features has expanded huge approval over multiple-factor validation. Several other physical modalities, such as fingerprint, face biometrics, and Face detection-based applications, have had many applications for years. The face is a distinct modality, and humans classify it separately according to facial features. As a person’s identification using a facial feature is attained over the naked eye, face biometrics and face PA detection have been accepted for identification platforms and security-based applications, such as border mechanism developments. At the same time, FR systems are broadly fixed for reliable identification of a person as well as recognition. It also meets threats because of many attacks with high spots of Face PAD's openness. PAs, adversarial and imposter attacks are specific attacks that threaten PAD performance's consistent face. Furthermore, these attacks are face-morphing attacks, and this type of attack efficiently creates the FR model vulnerable. This section defines several existing types of research regarding face detection methods, tools, and models. These investigations offer a suitable method to invent an accurate model or method for face detection. In 2022, Faseela Abdullakutty [9] described presentation attacks as a dangerous risk to one of the more common authentication domains, such as face recognition. In previous years, several approaches were utilized to detect and recognize these attacks with openly accessible datasets. But, these datasets were frequently composed in controlled atmospheres and concentrated on one specific attack category. The authors hypothesize that a model's perfect presentation on more than one existing dataset did not automatically security simplification through further, undetected face presentation attacks. The authors proposed a tentative structure where the generality capability of preliminary qualified deep models was evaluated with four widespread and frequently utilized datasets. Several permutations of these datasets accepted the broad trials and an outcome of the proposed framework presented with better performance. But, the composition of openly available datasets and models might still not be accomplished to simplify hidden attacks. In 2022, Zhigang Yu [10] described FR as advanced technology that offers various applications in different areas. Several existing models studied, which was truly carried wide accessibility in aspects. The authors proposed an innovative GoogLe_Net-M network for the FR method. That improved the performance based on network restructuring. The accuracy of the proposed model was improved by regularization and migration learning approaches. An efficient result of the proposed Google_Net-M network was reached better, such as recall rate (0.97) and accuracy (0.98) by using the above-mentioned learning methods. The cross-entropy evaluated the loss function by using eq (2.1) in this eq, C1 = output, y1 = expectation, and a1 = reality. The training procedure encountered the issue of higher and low training performance, overfitting defined in eq(2.2).

$$C1 = \frac{1}{n}\sum_{x} \quad [y1\,Ln.a1 + (1 - y1)Ln(1 - a1)] \quad 2.1$$

$$L = C1 + \frac{\lambda}{2n}\sum_{w1} \quad w1^{2} \qquad 2.2$$

In 2021, Arbena Vishi and Blerim Rexha [11] described biometric authentication approaches demonstrating the 'somewhat you are' pattern. That was considered the best-protected method for attaining entrance to threatened resources. Current outbreaks with ML methods demand a severe efficient revision of biometric verification**.** The authors developed a fast gradient sign (FGS) method using FR for biometric identification. In 2021, Artur Costa, Daniel Pére, David Jiménez, José Luis Alba, and Esteban Vazquez [12] described FR technology advancing currently adequate to utilize portable devices, such as smartphones, PC, laptops, or tablets. But, these devices were required due to a lack of better robustness against fraud or imposter attacks. So, the authors developed a face-PAD model named GRAD-GPAD, which was a holistic estimation model. A widespread solution of the generalization issues resolved in face-PAD combined with an estimation policy constructed on openly accessible datasets and collection of different protocols. That covered the maximum accurate backgrounds with an original demographic-biased study. An innovative fine-grained classification of PAs and mechanisms was delivered as better flexibility during the evaluation of the simplification-based methods. The proposed GRAD-GPAD offered to estimate the face-PAD method's performance in genuine backgrounds, supporting liability and unbiased evaluation of most face-PAD methods. In 2022, Azeddine Benlamoudi [13] described the face recognition approach as the most commonly recycled method for authenticating a person's characteristics. But, it was augmented in acceptance, raising alarms regarding face PAD attacks, in which a picture or audio-visual of an official individual's face was required to contact the service station. The authors constructed on a permutation of background subtraction or contextual elimination method using a CNN, and a collaborative classifier. They proposed an effective and supplementary robust face attack recognition method. The proposed method included a fully connected layered classifier through an MV (majority vote) method, which required several face PAD attack tools such as spoofing and replayed video. The suggested technique expressively boosts the recital of the FAS (face anti-spoofing) model. The authors utilized several databases and achieved an HTER of 0.62% and an EER of 0.58%. In 2022, Ziwei Song [14] described the WHO face masks as more effective safeguards from transferrable airborne illnesses, such as COVID-19. Subsequently, the spread of transferrable airborne illnesses and diseased countries enforced strict mask instructions for interior companies and open places. Although wearing a mask was required, the situation and form of the cover must be careful to raise the usefulness of face masks, exclusively in detailed unrestricted localities. But, it was very hard for the conventional facial detection approach to recognize entities designed for security authorizations. To resolve this difficulty, the authors proposed a spartan facial detection and face recognition method with DL methods required to protect the four most important subjects: mask recognition, identity detection, mask form, and mask location classification. Several models and Facial Recognition Pipelines through the face net were the DL procedures utilized to organize the features in every development. The proposed method was driven through five mechanisms counted preparation stage, server, supportive agendas, hardware, and manipulator interface. Real entities trials use cases, and predicted outcomes were used to estimate and predict the model's presentation. The model offered cost-efficient facial recognition and detection through mask resolutions for initiatives and institutes that can be realistic on control devices.

III. MATERIAL AND METHODS

The proposed framework in this research article used an improved feature selection-based MSVM classifier to detect the FPA and compared it with pre-trained models such as Vgg-16, ResNet-50, Inception V3, DenseNet-121, etc. NUAA [15] database widely defined public database.

A. NUAA Database

NUAA [15] Dataset is the major openly accessible face PAD database designed for printed photograph attacks. It contains certain inconsistencies in the presentation attacks, as the photographs are stimulated or biased in visible of the presentation attacks gaining method. A generally captured device such as a webcam is utilized for footage of the unaffected face imageries and around 15 matters were registered in the dataset. Also, every matter was examined to escape eye irregularity and save a forward posture, using an unbiased facial appearance. The attacks are accomplished through printed pictures. The dataset is distributed into separate twofold subdivisions: for preparation and analysis. The facial descriptions remained and then re-dimensioned to 64 * 64 pixels. Abstracts from the NUAA dataset are presented in Fig 1.

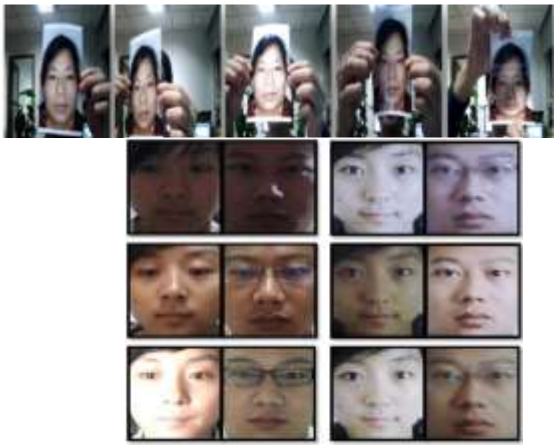


Fig 1. NUAA Image Imposter Face Database [15]

The no. of images in each class conforming to different databases and the combination database is defined in Fig 1 and Table I. Fig 1 represents the distribution of real and fake categories in the separate and data-aggregated database is defined. NUAA database has equal no. of real and fake category images in the training set.

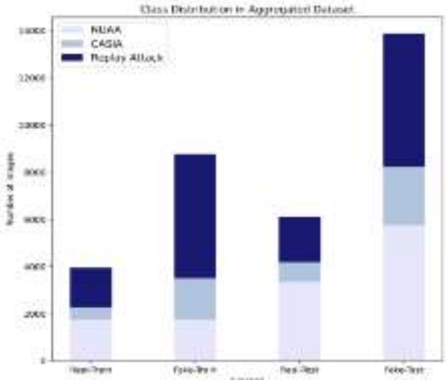


Fig 2. Class Division in Database

TABLE I.
NO. OF REAL AND FAKE IMAGES IN DATABASES

Database	Train		Test	
	Real	**Fake**	**Real**	**Fake**
NUAA	1743	1748	3362	5761

B. Methods

The face PAD system defines the legitimacy of perceived faces and contains image classification. With improved feature selection-based, the MSVM model has a combination of two methods such as GWO optimizer, and MSVM classifier. The proposed model, the face PAD system has also attained important enhancement, same to any other CV task. Through, that improved feature selection-based MSVM classifier needs a considerable quality of data to attain desired performance. To resolve issues, ML has been increasingly famous. In this proposed method, a task may be proficient with minimum training data, and time, and with maximum accuracy rate. The popular of the face anti-spoofing database is restricted in size. As an outcome, ML was used to reduce these challenges.

The complete process of the planned improved Face PAD model is described as a flow chart in Fig. 2. The proposed steps are defined with an improved feature selection-based MSVM classification model.

1. Train Dataset (Knowledge-Based Domain)
2. Test Dataset
3. It converts RGB to grayscale format.
4. It includes artificial Noise
5. After that, it applied the filtration method.
6. Edge detection
7. SIFT method using Feature Extraction
8. GWO method uses feature Selection and classifies the PAD face image.
9. It calculates the proposed model performance metrics.
10. Comparison.

Step 1:- Upload Dataset: It explores the dataset from the online repository site (NUAA). It has downloaded and trained the database according to the classes such as real and PAD attack images. It creates a knowledge domain with the help of an improved feature selection-based MSVM classification model. It has uploaded the image from the trained folder.

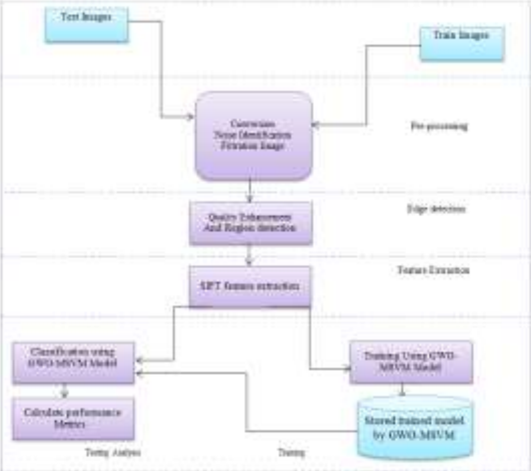


Fig 3. Proposed Flow Chart

Step 2: Pre-processing: It has applied the step i.e., RGB to grayscale format. The grayscale conversion step has been used to reduce the dimensions of the uploaded train RGB image.

Step 3: Filtration and Edge Detection Method: It has developed the filtration method to identify the noise in the uploaded image. The noise attack means to damage the input face image. So, noise level identification has developed a filtration approach to evaluate the filter image. After that, the filtration procedure implemented an edge detection technique to fetch the ROI of the specific object which is the face area.

Step 4: Feature Extraction (FE) Method using SIFT: It has implemented SIFT approach which is used to feature extraction. It reduces the image content to a set of points utilized used to detect the same designs in other images. This method is normally regarded as CV (computer vision) uses, adding image matching and object detection. SIFT KPs of objects are initially removed from a set of uploaded images and saved in a dataset. An object is predictable in a novel image by separately linking each feature from the novel image to this dataset and searching candidate matching feature-based on the ED (Euclidean distance) of their FVs (feature vectors).

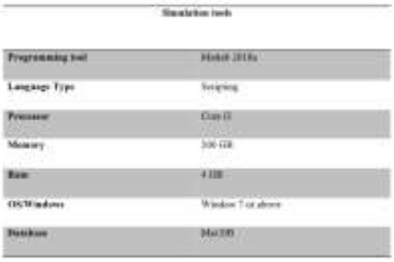
Step 5: Improved feature selection-based MSVM classification model (GWO+MSVM): This procedure uses a hybrid approach that has been designed using the grey wolf optimizer and MSVM classifier method. The optimization step has selected the feature sets based on extracted feature sets and classified the presentation attack face images. It classifies the feature vectors based on the MSVM classifier model has calculated the minimum distance and verifies the presentation attack and actual face images.

*Step 6: Calculate Performance Parameters :*It calculates the performance examination with the help of accuracy, HTER, and error rate, and compares it with the existing approaches.

IV. RESULT ANALYSIS

The simulation required essential tools and system requirements to process and analyze the proposed models and face PA detection from the dataset. Table II shows the minimum requirements of the given devices and platforms.

TABLE II.
SIMULATION TOOL



Simulation tools	
Programming tool	Matlab 2018a
Language Type	Scripting
Processor	Core i3
Memory	500 GB
Ram	4 GB
OS/Windows	Window 7 or above
Database	MatDB

A. Statistical Analysis

In this section, describe the performance parameters required for the proposed Face PAD system. That is defined as;

- *MSE (mean square):* It calculates the number of errors in arithmetic models. It evaluates the average squared variance between the detected and predicted weights. The value of MSE is set at zero when a system consists of no error. More errors in the model increase its value. It is represented in eq(i):

$$MSE = \frac{1}{N}\sum_{i=1}^{n} \quad (f_i, x_i)^2 \ldots\ldots\ldots\ldots\ldots\ldots(i)$$

- *Accuracy Rate:* It is defined as the total sum of TN (true negative) and TP (True Positive) divided into the total sum of TP (true positive), TN (true negative), false negative (FN) and Fase positive values. It is represented as eq (ii);

$$Accuracy = \frac{TN+TP}{TN+TP+FN+FP}\ldots\ldots\ldots(ii)$$

- *FAR (False Accept Rate):* It is defined as a numerical degree used to define the probability of a biometric safety model permitting illegal user entrance. It processes the fraction of unacceptable inputs which are wrongly recognized. It is represented as eq (iii);

$$FAR = \frac{FN}{TP+FN}\ldots\ldots\ldots\ldots\ldots\ldots\ldots(iii)$$

- *FRR (false reject rate):* It is the fraction of FP (false positive), and the sum of FN false negative) and FP. It is represented as eq (iv);

$$FRR = \frac{FP}{FP+FN}\ldots\ldots\ldots\ldots\ldots(iv)$$

- *HTER (Half Total Error Rate):* It is defined as the total sum of FAR and FRR divided by 2. It is represented as eq (v);

$$HTER = \frac{FAR+FRR}{2}\ldots\ldots\ldots\ldots\ldots\ldots\ldots(v)$$

B. Results

This phase described the resulting outcome with an improved feature-based MSVM classifier model to detect the presentation attack face image. The knowledge domain has trained several dataset face images from the train folder. It uploaded the images from the train folder. It applied the preprocessing image step, feature extraction (FE) approach to extract the reliable features and classify the improved feature-based MSVM classifier model and attack the face images and detect the actual and fake images. The testing phase is generally analyzing the test image as compared with the training phase or a dataset. Test analysis with improved feature-based MSVM classifier models and test the feature vector with train database feature vectors. If the train feature has been compared with the test feature vector and then evaluate the neighbor feature set. It calculates the feature vector and analysis the actual face image and attacks face images.

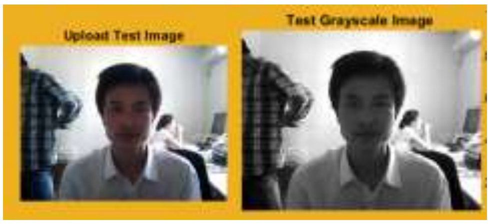


Fig 4. Input and Converted the image

Fig 4 defines the upload of the test input image from the test folder. It interchanges the color image into a gray-scale image. It mitigates the sizes of the uploaded input image. It uploaded the three-dimensional image and RGB to the grayscale command implemented and extract the image black and white image format and two-dimensional format.

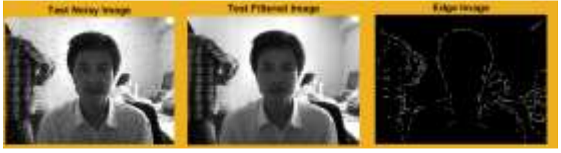


Fig 5. Preprocessing Outcomes

Fig 5 defines the noisy image using salt and pepper. A filtration process has been useful to mitigate the noise data with the median 2d transformation method. After that, the edge detection system uses the Prewitt operator. It creates an image emphasizing edge evaluating an approx. of image gradient and integer value filter in the instructions such as horizontal and vertical. So, comparatively cheap in terms of evaluations.

Below Fig 6. defines the feature extraction using SIFT method. This method has reduced the image content to a set of points utilized to detect the same patterns in other face images. This method is normally regarded as CV uses, adding image matching and OD (object detection).

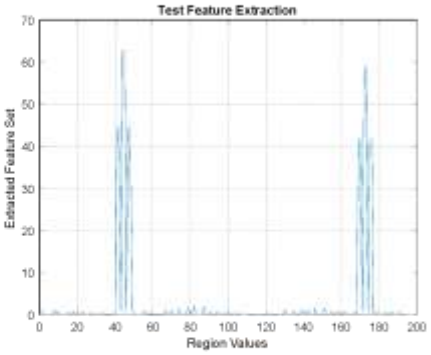


Fig 6 Feature Extraction Using SIFT Method

This approach is motivated to optimize the no. of features in the database by passing them through an MF (mapping function). An image's KPs (key points) are spatial positions that are rotation and scale-invariant. These KPs highpoint what stands out in an image and that pixels are of utmost significance. Descriptors are vectors that define the local surroundings around the KPs present in the image. These descriptors are utilized to make connections among different face images.

Fig 7. Detected Category

Fig 7 defines the Improved feature selection-based MSVM classification approach. It is prepared with a gathered of random feature sets and then explores for best optimization by informing groups. The individual round feature is efficient by subsequent two BVs (best values). MSVM classifier models are attractive because they have neighbor solutions that can be easily evaluated are inherently multiple classes have defined. It defines that the PAD face is based on train and test feature vectors. If the test feature vector is compared with the existing train feature set the neighbor value to evaluate and it calculates the distance and detects whether the PAD faces an attack or not.

Below fig 8 defines the HTER performance with the proposed model. The HTER (half total error rate) is a performance parameter normally utilized in BS, like FR. It calculates the overall ER (error rate) by considering both the FAR and FRR. It enhances the FS (Feature selection) based MSVM classifier model for optimizing the HTER, it can follow the steps mentioned earlier for FS and training the MSVM classifier. The proposed model to incorporating FS and optimizes the model to reduce the HTER. The performance of the EER (equal error rate) with the proposed model using an improved feature selection-based MSVM classifier model. EER rate is generally utilized parameter in BS (biometric systems) to calculate the performance of face PAD methods. It calculates the point at which the FAR and FRR are equal. The FAR defines the rate at that imposters are inaccurate as real, while the FRR defines the rate at that real users are accurately rejected. It evaluates the EER rate for face PAD, it generally required a database with a combination of real access attempts and PAD (Spoof attack). The database should add a sufficient no. of samples for both categories.

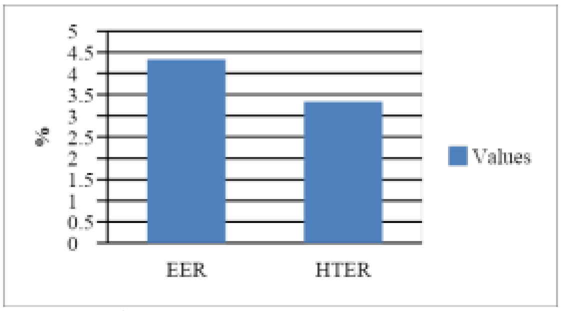


Fig 8. Performance Analysis with proposed model (HTER, and EER)

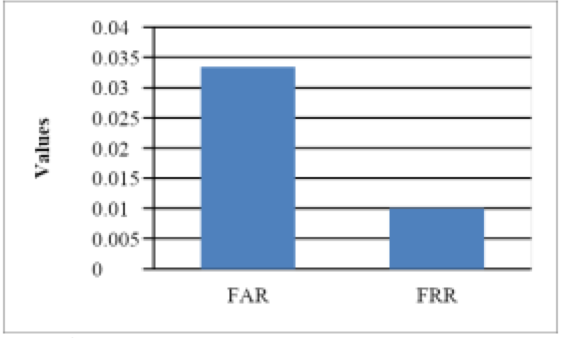


Fig 9. Performance Metrics with the proposed model (FAR and FRR)

Fig 9 shows the FAR as a crucial parameter for calculating the presentation of FPAD systems in the context of FR (face recognition). It defines the rate at that PAs (presentation attacks) are inaccurately accepted as real users. It calculates the FAR for FPAD, it required a database that adds real face images and PA images. The database should cover a broad range of scenarios and PA categories. It defines the proportion of PA attempts that were inaccurately classified as real. A minimum FAR defines a more robust and precise FPAD system. FRR is a critical parameter used to calculate the performance of FPAD systems in the context of FR. It defines the rate at which real users are incorrectly rejected as PAs. It evaluates the FRR rate for FPAD, it required a database that adds both real face images and PA images. The database should cover a wide range of scenarios and PA classes.

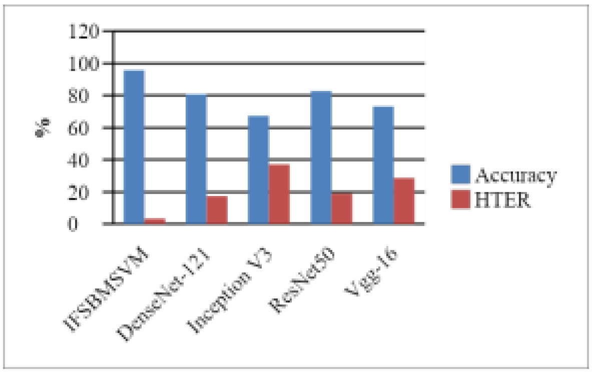


Fig 10 Comparison Analysis

Fig 10 and Table III show the comparative analysis with proposed and existing models such as IFSBMSVM, DenseNet-121, inception V3, ResNet-50, and Vgg16. The proposed model has improved the 95.6 percent accuracy rate as compared with the existing models. The proposed model has reduced the half total error rate as compared with the existing models.

TABLE III
COMPARATIVE ANALYSIS

Models| Parameters	IFSBM SVM	DenseNet-121	Inception V3	ResNet 50	Vgg-16
Accuracy	95.66	80.7	67.4	82.60	73.10
HTER	3.33	17.40	37.0	19.0	28.41

V. CONCLUSION AND FUTURE SCOPE

In proposed work has concluded and used the NUAA dataset. In the knowledge-based train, the images and proposed approach are based on the improved feature selection-based MSVM classifier. It proposed a model that depends on the chosen unique features and fetched feature sets from the facial images. A Prewitt edge operation is used to evaluate the face edges based on the inner and outer fields. SIFT method is utilized for the feature extraction method to calculate reliable feature sets. The GWO (grey wolf optimization) approach is used to choose the feature set established on the FFn (fitness function). It is fetching the reliable solution in the extracted feature set value. IFSBMSVM classifier has been implemented to identify the train and test feature vector and calculates the nearby distance. It compared the neighbor feature vector and feature assessment true, then calculate the performance parameters such as an accuracy rate value of 95.66 %, HTER value of 3.3 %, and compared with the existing methods.

Further improvement will extract the local and global feature sets and implement a HAAR wavelet transformation method used to filter the face presentation attacks in online face images. It will enhance the processing time, optimize the complexity, and attain will high accuracy rate.

REFERENCES

[1] Singh M, Singh R, Ross A. A comprehensive overview of biometric fusion. Information Fusion. 2019;52:187–205.

[2] Ramachandra R, Busch C. Presentation attack detection methods for face recognition systems: a comprehensive survey. ACM Computing Surveys (CSUR). 2017;50(1):1–37.

[3] Zhang Z, Yan J, Liu S, Lei Z, Yi D, Li SZ. A face antispoofng database with diverse attacks. In: 2012 5th IAPR International Conference On Biometrics (ICB). IEEE; 2012. p. 26–31.

[4] Jia S, Guo G, Xu Z. A survey on 3D mask presentation attack detection and countermeasures. Pattern Recogn. 2020;98:107032.

[5] Chingovska I, Anjos A, Marcel S. On the effectiveness of local binary patterns in face anti-spoofng. In: 2012 BIOSIG-Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG). IEEE; 2012. p. 1–7.

[6] Määttä J, Hadid A, Pietikäinen M. Face spoofng detection from single images using micro-texture analysis. In: 2011 International Joint Conference On Biometrics (IJCB). IEEE; 2011. p. 1–7.

[7] Patel K, Han H, Jain AK. Secure face unlock: spoof detection on smartphones. IEEE transactions on information forensics and security. 2016;11(10):2268–83.

[8] Komulainen J, Hadid A, Pietikäinen M. Context based face anti-spoofng. In: 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS). IEEE; 2013. p. 1–8.

[9] Abdullakutty, Faseela, Eyad Elyan, Pamela Johnston, and Adamu Ali-Gombe. Deep Transfer Learning on the Aggregated Dataset for Face Presentation Attack Detection. *Cognitive computation* 14, no. 6 (2022): 2223-2233.

[10] Yu, Z., Dong, Y., Cheng, J., Sun, M., & Su, F. Research on Face Recognition Classification Based on Improved GoogleNet. *Security and Communication Networks*, *2022*, 1-6.

[11] Musa, A., Vishi, K., & Rexha, B. Attack analysis of face recognition authentication systems using fast gradient sign method. *Applied artificial intelligence*, *35*(15),2021, 1346-1360.

[12] Costa-Pazo, A., Pérez-Cabo, D., Jiménez-Cabello, D., Alba-Castro, J. L., & Vazquez-Fernandez, E. Face presentation attack detection. A comprehensive evaluation of the generalization problem. *IET Biometrics*, *10*(4), 2021, 408-429.

[13] Benlamoudi, A., Bekhouche, S. E., Korichi, M., Bensid, K., Ouahabi, A., Hadid, A., & Taleb-Ahmed, A. Face Presentation Attack Detection Using Deep Background Subtraction. *Sensors*, *22*(10), 2022, 3760.

[14] Song, Z., Nguyen, K., Nguyen, T., Cho, C., & Gao, J. Spartan face mask detection and facial recognition system. In *Healthcare* (Vol. 10, No. 1, p. 87), 2022. MDPI.

[15] Hernandez-Ortega, Javier, Julian Fierrez, Aythami Morales, and Javier Galbally. Introduction to face presentation attack detection. *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection* (2019): 187-206.

[16]Hardeep Singh Saini, Dinesh Arora and Manisha Verma, An effective audio watermarking approach with high data embedding, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol.8, No.4S2, pp. 185-190, 2019. https://www.ijitee.org/wp-content/uploads/papers/v8i4s2/D1S0038028419.pdf

[17]Ramandeep Kaur, Abhishek Thakur, Hardeep Singh Saini, Rajesh Kumar, "Enhanced steganographic method preserving base quality of information using LSB, Parity and spread spectrum technique", 5th IEEE International Conference on Advanced Computing & Communication Technologies (ACCT- 2015), was held on 21-22 Feb.2015 at Rohtak -Haryana-India, pp.148-152. . doi.10.1109/ACCT.2015.139

[18]Ajay Kaliraman, Abhishek Thakur, Hardeep Singh Saini, Rajesh Kumar and Naveen Kumar, "Speech Enhancement by End Point Detection and Signal Subspace Method", 2016 IEEE First International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), 978-1-4673-8587-9, 4-6 July 2016 at Delhi Technical University, Delhi. **DOI:** 10.1109/ICPEICES.2016.7853239.

[19]Manish Kansal, Dinesh Arora and Hardeep Singh Saini, FPGA Implementation of FIR Filter used for DSP using Matlab&Modelsim, International Journal of Electronics Engineering Research (IJEER), ISSN: 2230-7109, 3(3), pp.363-373, 2011.

https://www.ripublication.com/Volume/ijeerv3n3.htm