MACHINE INTELLIGENCE RESEARCH
ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

OPTIMAL FACE SPOOF DETECTION BASED ON IMPROVED WHALE OPTIMIZATION ALGORITHM AND DUAL STAGE CONVOLUTIONAL NEURAL NETWORK HYBRID

[1]Mukesh Madanan, [2]Nurul Akhmal,[3]Nitha C. Velayudhan
[1,2]Department of Computer Science, Dhofar University, Oman
[3]Universal Engineering College, Kerala, India
mukesh@du.edu.om, nzulkefli@du.edu.om, nithacvelayudhan@gmail.com

ABSTRACT

Face detection systems are now being utilized in various application systems, for instance, periphery crossing points, banks, and security information access etc. Advanced facial verification systems can focus on the vulnerability of facial biometrics to process swindlers and use photos, videos or 3D nodes of verified customer faces to create access to the workplace or system and important secured data. Facial correction or dynamic differential correction algorithms (e.g., face activation or deception selection) could be utilized in solving such a crisis of deception. Adversely, the current issue is due to the difficulty in the detection of bias and computation anomaly intrusions. The paper proposes an optimal face spoof detection (OFSD) methodology along with artificial intelligence framework for the spoofing detection procedure. Initially the methodology of proposed OFSD design begins with a dual stage convolutional neural network (DS-CNN) managing different comparisons of space information for face spoof recognizable proof. Secondly, an improved whale optimization algorithm (IWOA) streamlining estimation for feature classification to select best perfect features from various level is utilized. Subsequently an optimal rule based fusion (ORBF) procedure for sufficient interweaving of the features from different sources is structured. Exploratory analysis of three publicly available databases, REPLAY-ATTACK, CASIA-FA and OULU-NPU, reveals interesting results that differ from previous work.

Keywords: Optimal rule based fusion, Optimal face spoof detection, IWS, DS-CNN, Biometrics, Face recognition.

1. INTRODUCTION

Facial stability is the most efficient and comprehensive application feature of various biological aspects in comparison to fingerprint, iris separation, and hand shape. This feature recognition method is conventional and sturdy [1] [2].The features can be categorized to predefined features for recognition and interactive features. The real pre-requisite to rely on sustainable artificial intelligence techniques is to attain a facial image and perform critical learning in the beginning [3]. In addition to this, the effortlessness of using and blending of facial biometric systems introduces several issues with the security. Moreover, when we consider facial affirmation, a noteworthy concern develops with respect to trustworthiness. This could be a situation where one individual endeavors to procure access as another person by using facial identification of a real person. The concern here is the liveness acknowledgment of a facial picture. This means choosing whether there is really a living individual before a camera and not an undertaking to character distortion by presenting a photo or a video in order to get unseemly access [4][5]. Consequently, it is typical that a face anti-spoofing (FAS) technique should have the option to perceive an image that does not have an intrusion detection in contrast to the one that has it. Henceforth, a given course of action must have the choice to get pictures captured from various sources and play out the gathering of these photos as genuine or counterfeit [6].

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

In spite of all the various accomplishments of facial certification, it has been observed that some ambushes occur because of the inescapability of online life from which facial pictures are certainly not difficult to get. For example, an introduction assault can record an individual's face data by printing it, repeating it on screen, or, in any case, generating the face using techniques like 3D covering and VR, which raises a slew of testing security concerns [7]. Security worries of face confirmation structures have various appraisals for face deriding disclosure. From the point of assessing the disturbing effect data infused into the scrutinizing media to the development of various approaches to target evacuating the mutilation data may show up on animation face which tests a series of events that occur [8][9]. Conventional deriding knick-knacks solidify surface outdated rarities, advancement of old pieces and picture quality relics etc. Distinct approaches based on the framework level in which unequivocal sensors are used for extra rigging can be interwoven into the assertion structure (e.g., infrared sensor) [10].

Using Artificial Intelligence estimations and predictions to deal with the issue of face liveliness disclosure requires cases of affirmed pictures and misdirecting pictures. In order to see the face scrutinizing with multiple options such as covering surface appraisal, joint camouflaging surface data and knowledge from the luminance and the chrominance channels by evacuating correlative low-level fragment depictions from non-identical concealing spaces, a partner with structure was used by Boulkenafet et .al[11]. A sensible obvious check system subject to the evaluation of picture bends in 2D spoof face pictures and the essential of independent signs was employed by K.Patel et al[12]. H.Yu et al employed a channel bank based cepstral join that has gigantic neural structure channel bank cepstral coefficients to see trademark and phony talk [13]. A solid foe structure for the face liveness undeniable proof with morphological errands subject to eye blink and mouth redesigns for expanding most basic steadfastness during face liveness insistence was proposed by Singh and Arora [14]. A bewildering depiction together showing 2D calculated information and similarity information is used for face detection against caricaturizing technology. The printed merge is obtained from 2D facial picture locale using a Convolutional Neural Networks (CNN), and the broad depiction is expelled from pictures obtained by a Kinect [15]. An assertion system relies on the blend of surface deployed procedures and picture quality assessment estimation techniques [16]. Three sorts of assertion solidify vectors are LBP, DoG and HOG with and without feature affirmation systems, for instance, PCA and LDA. A persuading and non-bursting system to counter face-taunting ambushes that uses a single picture to perceive caricaturizing attacks subject to an additional substance head confining to course of action was introduced by Alotaibi and Mahmood[17]. Xia et al researched the extraordinary etching liveness confirmation as a two-class gathering issue and proposed a model based on noteworthy etching liveness region framework that achieves unbelievable obvious check precision [18]. The confirmation execution employing live faces and normal quality fake face records that showed contraptions using the introduction openings among live and fake faces under remarkable lighting settings to demonstrate if the engine is adequate or not was studied by Cho and Jeong [19]. De Souza et al recommended a two LBP-based CNN, LBPnet and n-LBPnet, for caricaturizing revelation in face affirmation structures, which achieves astonishing results on the NUAA disdaining dataset, squashing other investigated top-level systems [20].

The research work proposes an optimal face spoof detection (OFSD) based on hybrid machine learning technique and Improved whale optimization algorithm (IWOA). The main objective of proposed OFSD design is:

- To introduce a novel machine learning technique to handle and detect illumination problems.
- To introduce optimization algorithm for feature selection process, that can effectively capture the complementarily of two features.

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

- To design optimal fusion method for effectively fusing the features from different sources.

The section 2 describes the existing techniques prevailing in face detection. Additionally, section 2 discusses the problems with face detection and the current solutions. The proposed spoofing face detection method is purported in section 3. The empirical data and debates are described in Section 4, and the conclusion is offered in Section 5.

2. LITERATURE REVIEW

Chan et al. [21] suggested a face liveness recognizable proof strategy with streak against 2D ridiculing attack. The streak not only can improve the detachment among valid and askew users, it can also lessen the effect of natural components. Four surface and 2D structure descriptors with minimal computational properties are used to obtain information about the two images in the model. The focus of their strategy was to fix the low base value To analyze the proposed method, Chang et al. used 50 subject data collected under different conditions from the initial condition.

For the depiction and assertion of dynamic surfaces, Zhao et al. [22] offered a close by spatio-short lived descriptor, to be explicit, a volume local binary count (VLBC). In order to show a dynamic surface, the Volumetric Local Binary Pattern (VLBP) isolates histograms of threshold near by spatiotemporal volumes utilizing both appearance and development criteria. VLBC does not obstruct information about nearby structures; it merely examines the number of threshold codes. Therefore, like VLBC, we can combine pixels around Visible Light Photon Counters (VLPC) without significantly expanding the component count. Complete adjustment of the VLPC (CVLPC) was proposed to improve the visualization of dynamic surface stability with more information on the separation and proximity of the central pixel force. The proposed strategy not only creates the table, but also provides dynamic surface imaging.

Moghaddam et al. proposed a strategy for ambiguous cameras [23]. The IST Lenslet Light Field Face Spoofing Database (IST LLFSD) simulates six different spoofing attacks, inclusive of printed paper, wrapped paper, a PC, a tablet, and two distinct mobile phones [23]. Dangerous crime presentation is an inadequate but informative story that combines curtains and surfaces with other light paths captured from light field photos.

Edmunds et al. proposed an anti-spoofing approach that will derive features, which are discriminant [24]. The method is driven by enrolment data, which is used for creating specific set of 12 features. These set of features encapsulated the variance between artefacts and real face. The research successfully and reliably recouped the radiometric discrepancies between real face and face artefacts. The main drawback of the research highlighted was that the method does not distinguish color distortions. These distortions occurred due to variations in the illumination process and sometimes waived off due to the colour distortions when the pictures were recaptured.

Li et al. put forward a novel framework highlighting the ability of deep learning in conjunction with domain generalization [25]. The research contemplated the spatial and temporal information for proposing a 3D CNN architecture. Facial samples were used to train the model that were created based on cross entropy and these were used for the learning features to create a generalization and classification. By reducing the maximum mean discrepancy, the researches employed a generalization regularization.

Zhang et al. [26] have introduced a face mocking divulgence conspire subject to Color Texture Markov Feature (CTMF) and Support Vector Machine Recursive Feature Elimination (SVM-RFE). The pixels around the face investigate the distinctions between symmetric and pseudo-facial expressions on various pillars and propose the CDMF, CCMF, and CCDMF face lamps. In fact, each channel can handle facial data. SVM-RFE was used to minimize area estimation and to ensure the accuracy and consistency of the area. By applying image codes at different distances, some face-to-face data can be applied to the cross space in the disguise of the CDMF, and can be designed to gradually create exaggerated area schemes

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

with different surface highlights.

Rehman et al. [27] have proposed a productive way for face liveness divulgence when the preparation information is restricted. This methodology uses consistent data randomization rather than normal bundles during setting up a CNN architecture. This structure diminishes arranging time generously by methods for setting up the system in limited and sporadic gatherings. The information randomization approach looks like bootstrapping structure, which is completely possible in envisioning the class of obscure models utilizing little degree individuals for preparing.

Beham et al. [28] have proposed a system subject to aggregated local weighted grant orientation (ALWGO) inspired by depth map estimation. To estimate the form of the model face picture, discriminant ALWGO features are disengaged from the significance map. An outline classifier is established to observe the guaranteed and fake appearances. These particularly addressed the limit of surface tendency features and their assortments on three types of ambushes. These are the printed top quality photographs, warped photographs and mobile phone videos played on it. The utilization of ALWGO features has been elevated for further recognition of facial features.

Kavitha et al. [29] have proposed multimodal bio-structures to detect a fake face from a real face. The EDGHM-Surf description were integrated with the face image functions HSV and YCBCR masks. This method was employed for everything from behavioral settings to severe spot score IDs and severe abuse and testing. Nevertheless, this method does not permit accurate stick responses in the field. Attached functionality is performed on the k-SVM classifier to identify duplicates.

Rehman et al. [30] made an important contribution by proposing a solid sound structure based on a camera-based face liveliness area technique that employs dynamic qualification maps derived from convolutional-highlights with stereo-pair camera face images. The assorted kind of uniqueness were obtained with the maps picked up from convolutional-highlights stereo-pair camera face pictures, for example, the absolute disparity (AD), feature multiplication (FM), the approximate disparity (APD) and square disparity (SD). The magnitude map estimation method utilizing the stereo-pair camera is a working appraisal subject to PCs vision, and since current top level CNNs have been demonstrated to be possible in making essential and qualification data for an assortment of errands, core CNN for stereo-pair camera face liveness region was considered. Besides this, the method investigates testing conditions for testing of stereo-pair camera based face liveness affirmation structures which will assist in surveying the theory and achievability of stereo-pair camera-based face liveness region frameworks constantly.

Regardless of the ways that exists face-ridiculing disclosure frameworks, face spoofing is a serious issue because they are efficient and difficult to detect using indigenous test tools. The presentation area is essential when expanding because it mainly uses the full image or the entire video in the expanded area. There is, in particular, a lack of assessment of how sharp the image matches to the spoofing's maximum image capabilities. In general, image areas are identified as redundant or confusing with the image, which reduces the visual and computational features of the object.

Li et al. [31] have suggested a procedure for face disdaining zone utilizing Local Binary Pattern (LBP) plan, which consolidates the hand-made highlights with noteworthy learning and can decrease the system parameters by getting the computer visions. Replay-Attack and CASIA-FA methods have demonstrated outstanding outcomes and accomplished stable results. These methods despite satisfying results have several limitations. This improves the visualization of some types of attacks and creates a highly sensitive database with high impedance. The influence of the static converter bit size and the reflected Locality Preserving Projections (LPP) is represented by different transition layers on the satirical side. Using partitions and other key gradient-based local structures, the parameters of the entire relational plot are related to 64x theory. After evaluating the two standard duplicate databases, Local Binary Pattern (LBP) integration uses the top-down methods Relay-Attack and Cassia-FA.

Two critical issues arise when face evaluation is taken into consideration. Certain cases of face evaluation

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

produced results with stunning quality for frontal pictures when the photographs are obtained two or three years or even some point later. One of the crucial issue is that it is hard to get a hand on an individual's outward appearance because of the developments of the face's appearance, illuminations, agitation, and nature of a picture. Additionally, the human face shields the most over the top data for seeing people. The face authentication has been broadly investigated and picked up stunning grounds in different applications in the prior decades. Despite the way that different techniques have been proposed for hostile to deriding, it has been found that the presentation of many existing procedures is adulterated by illuminations. To overcome these issues, this research proposes an optimal face spoof detection (OFSD) based on hybrid machine learning technique. The main contributions of proposed OFSD design are:

- A dual stage convolutional neural network (DS-CNN) to handle different complementary space information for face spoof detection.
- An improved whale optimization algorithm(IWOA) optimization algorithm for feature selection process, which compute best optimal features from different level.
- An optimal rule based fusion (ORBF) method for effectively fusing the features from different sources.

3. PROPOSED SYSTEM MODEL FOR OPTIMAL FACE SPOOF DETECTION

A systematic workflow of the prospective face spoofing detection approach is drafted in Figure. 1. Voluntary difficulties are created for individuals in order to check the face evaluation. This proposed technique is useful for detecting both the print and video playback attacks. The eye of person is very useful when repeating the structure and the DS-CNN based conversion is useful for both print and video playback attacks. Moreover, it is better to split the face into patches for evaluation rather than the whole face evaluation. Patches are the area of the eye, the nose, the lips, and the chin. The link classification can be extracted via DS-CNN to suit large amounts of information. Yield is the combination of sample scores for each error using IWS calculations. Developments and innovations are improving the DS-CNN, and it has been proven that both of these methods provide excellent results. If the combination of videotape scores is important for each error correction, a face-to-face image or video may be considered insignificant and will naturally be difficult depending on the client's response.

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

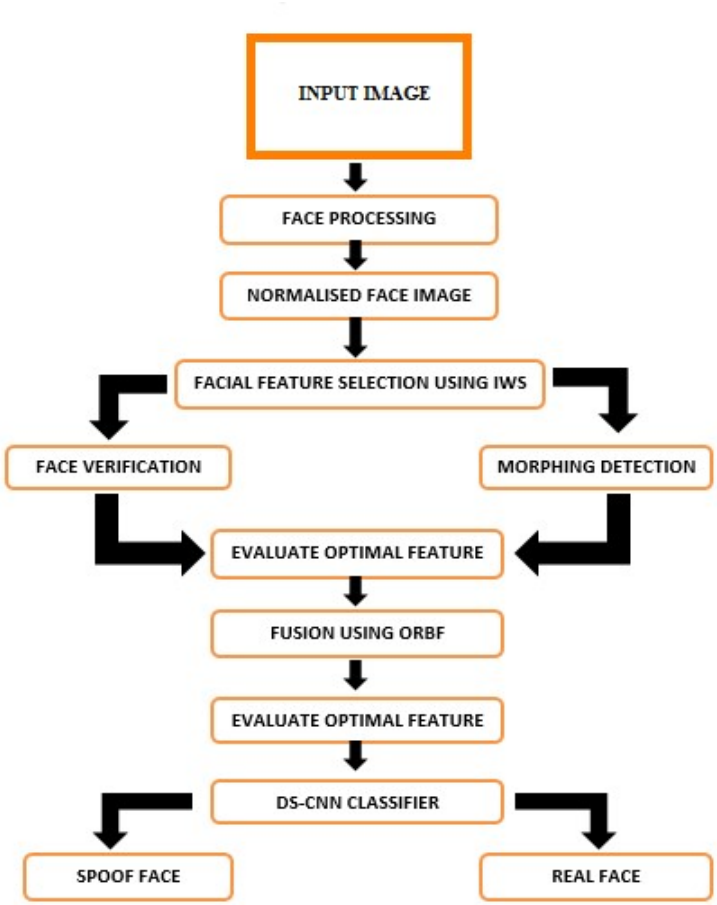

Figure 1. *Face spoof detection methodology - hybrid machine learning technique*

Two openly accessible element extraction calculations which accomplish results favorable in class execution on the Relay-Attack and CASIA-FA dataset were used. Subsequently, the classifier utilized in the investigations is portrayed.

3.1. Recognize with multi-layer perception using DS-CNN

Multi-layer perceptron is another name for a dual stage convolutional neural network (DS-CNN). A data layer, a transition layer, a pooling layer, a complete connection layer, and a yield layer make up a conventional neural network system. Because of this, the catalyst divides, pulls, and increases the accuracy required, which is usually associated with image and measurement. The result of a fundamental CNN is boosted to a figure that is dependent on the motivation that drives the net. For plummet into transgression, for instance, the yields may be used as they appear. For procedure, one could use the yields as obligations to an assistance vector with machining or sporadic woodlands or if the classifier requires input, it adds up to probabilities that yield stage that could be a softmax work. In this study, the structure of a classic neural system is modified, and a learning system with two veiled layers is proposed, as shown in Figure 2.

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

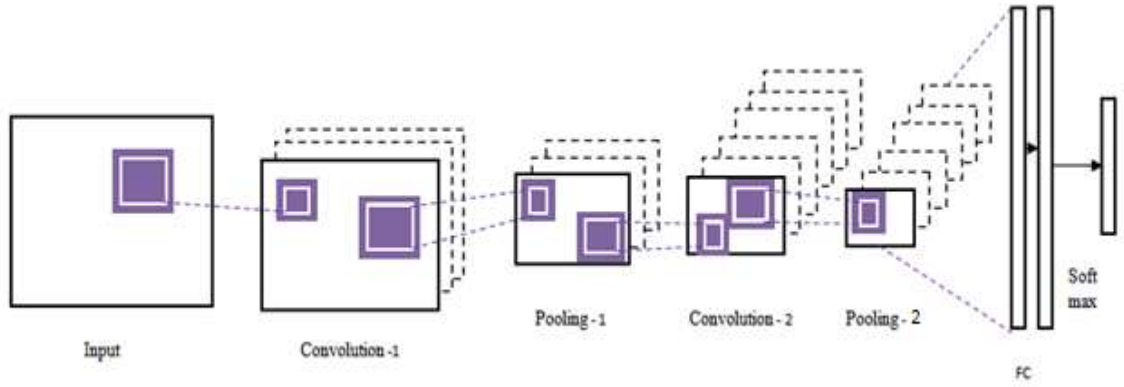

Figure 2.*CNN sequence to classify classroom source for IAQ*

Consider the equation

$$z \quad \sigma(y) = \frac{\exp(y)}{1^T \exp(y)} \tag{1}$$

where 1 is an area vector of ones. Dexterously, the exponential makes all totals positive, and systematization ensures that the segments of z suggest 1. Amazingly more authoritatively, past what many would consider conceivable can be seen as a multidimensional hypothesis is very far away from the certainty [1]. The motivation driving why this cutoff is referenced "softmax" is that on the off chance that one of the y_i sections, state $1^T \exp(y) \approx \exp(y_{i0})$, so that, $z_{i0} \approx 1 \quad and \quad z_i \approx 0 \quad for \quad i \neq i_0$, is from a general perspective more fundamental than a tremendous fragment of the others. Assuming the target that point so that the breaking point plausibly goes about as a pointer of the best passage in y. truly more convincingly, and clearly,

$$\lim_{\alpha \to \infty} y^T \sigma(\alpha y) = \max(y) \tag{2}$$

$$x(0) = x \tag{3}$$

$$x(l) = \pi(h(W^{(l)} \bar{x}^{(l-1)})) \quad for \quad l = 1,.....,L_c \tag{4}$$

$$x(l) = h((W^{(l)} \bar{x}^{(l-1)})) \quad for \quad l = L_c + 1,.....,L \tag{5}$$

$$y = h_y(x^{(L)}) \tag{6}$$

The character, softmax, or other breaking point could be the yield beginning work hy. D(0) = D and D(l) for l > 0 being relative to the measure of yields (or organizations) in layer number l, the frameworks W(l) have D(l) lines and D(l1) + 1 regions, with D(0) = D and D(l) for l > 0 being relative to the measure of yields (or organizations) in layer number l. The first Lc layers are convolutional, and the rest are all connected.

3.1.1. Data Input Layer

Pre-manipulated data with a single ID model are used as secondary data, the unique model estimate of type ID is 16000 × 1, and the hidden area is Principal Component Analysis(PCA). Data validation is predicted in the trademark subsection of 784 × 1, which reduces the learning benefit and computational aspects of complex learning structures.

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

3.1.2. Convolution Layer

The second protected learning method is mapped to the data by validating the estimation and partial extraction, thus converting the data from the reduced estimate into a test vector 28x28 structures. The basic transformation layer of the learning structure is derived from the 32, 5 x 5 transition part of the heuristic structure 1. The next Transformation Layer contains one of the 64 5 x 5 Transformation Pieces with experience. Integrated representation of layers as follows

$$Y_j^t = f(\sum_{i=1}^{M_j} w_{i,j} \times x_i^{l-1} + b_j^t),\ j = 1,2,.....N \tag{7}$$

in which, Y_j^t speaks to the j[th] highlight diagram of the l layer. $w_{i,j}$ speaks to the weight estimation of the convolution bit for the j[th] include diagram of the l layer and the i[th] highlight chart of l-1 layer; b_j^t speaks to the counterbalance of the j[th] include diagram of the l layer; N speaks to the quantity of the component charts of the l layer , f( ) speaks to the actuation work. The relu work utilized right now as follows:

$$f(x) = \max(0, x) \tag{8}$$

All neurons in a part map are required to have the same load; however, various segment maps within the same convolutional layer have varied loads, allowing a few features to be deleted at each territory the k[th] yield incorporate guidance Y_k. The profound investigation appears a casing acknowledgment, obtained from convolutional layer. This leads a significant job to CNN with different sort of channels to speak to a total casing. It maps a middle of the road property, and make distinctive area maps (Fig.2). It will do mapping from given information ascribe to shrouded layers. The information layer will pass the casing to concealed layer. What's more, it have three different hyper capacities to control the length of the yield layer in convolution. We additionally portrayed zero cushioning, profundity and walk. For instance, convolution accepting the information outline as info, and we referenced different neurons inside and out size may instate here,

$$Y_k = f(W_k * x) \tag{9}$$

b_{yx} is demonstrated as information outline; W_k is shown with kth trait, which like convolutional channel. It used to assess the pixel proportion of each and every edge and f( ) indicates the nonlinear trigger errand. Their picture and achievement have given to a zone of investigation that point out the progression and utilization of CNN activation abilities to improve a couple of characteristics of CNN execution.

3.1.3. Pooling Layer

The entire column, referred to as the Diagnostic Analytics tier, does not, however, reduce the area of data feature review or modify the size of the feature map in any way. The total layer required in our estimation is 2x2 channels and the moving length is 2 seconds, so the sample estimate is 14x14 after acquisition. Consequently, the entire layer uses 2 × 2 channels, and the operational length is 2, so after reviewing the second position, the sample has a rating of 7 × 7, is this layer a reasonable explanation

$$y_j^t = f(down(y_j^{t-1})) \tag{10}$$

in which, y_j^t , y_j^{t-1} represents feature diagram for L and L-1 plots. The bottom ( ) represents the sample functions below and the algorithm uses the maximum pooling function. f ( ) denotes a test operation using the relay function.

3.1.4. Full Connection Layer

This model is calibrated with map stability and pooling and separates useful functions for test simulation. Since the promise of the entire link layer is a one-dimensional region vector, the two-dimensional yield attribute coefficients of the top layer must be calculated by the location mechanism. Currently, the number

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

of neurons associated with the two columns is independent of 3164 and 1000, depending on the function map component of the top layer. The yield of each neuron

$$h_{w,b(x)} = f(w^T x + b) \tag{11}$$

in which, $h_{w,b(x)}$ marks the output of the neuron, the input eigenvector of the neuron is x, and the offset is b the Output Layer.

The output of the extracted function from the learning network is the input to the SoftMax classifier for output. The resulting model can be identified as a class. The signal sample set has a total of 8 classes, and class J determines the probability of the sample.

$$P(y^{(i)} = j \mid x^{(i)}; \theta) = \frac{\theta_j^T x(i)}{\sum_{l=1}^{K} \theta_i^T x(j)} \tag{12}$$

The model is calculated using easy classifiers in each class. Finally, the class label in the model determines which class has the highest probability value.

3.2. Feature Selection using IWS Optimization

Improved whale optimization algorithm(IWOA) optimization is a nature excited meta-heuristic headway estimation technique. IWS relies upon the pursuing behavior of humpback whales. In addition, IWS mimics the pursuing behavior of humpback whales using a winding air pocket net ambushing instrument to imitate the getting of prey (examination) and the use of a subjective or perfect request administrator to pursue the prey (examination) (misuse). Most Meta heuristics have an innovative technique that offers a common section. It is divided into two stages: abuse and examination. The continued and chasing action of humpback whales awakens improved whale optimization algorithm(IWOA). Humpback whales have a unique pursuing mechanism known as the air pocket net supporting technique, which entails forcing ascends along a to float around the prey while coasting around it.

3.2.1. Searching for prey

The searching is based on the vector A_n collection, and it is used to prompt request administrators to look for better options, such as an overall interest. The value of |A| is set to be greater than 1, allowing the pursuit authority to meander far into the interest space. In contrast to the abuse system, the interest administrators update their situation about a randomly selected request expert rather than assuming the best hunt master. Humpback whales filter for prey subjectively to the extent the circumstance of each other.

The numerical model can be depicted as pursues

$$D = | C.\omega X^*(t) - X(t) | \tag{13}$$

$$K(t+1) = X^*(t) - A \cdot D \tag{14}$$

where A denotes the coefficient vector, t denotes the current emphasis, X denotes the position vector, C denotes the coefficient vectors, a denotes the straight declining from 2 to 0, r denotes the arbitrary number between [0,1], and X* denotes the best estimate of the position vector. X represents a separate circumstance, and X^r and is a random number generated from the current

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

age that corresponds to a vector position, t represents the current cycle, the picture || represents the supreme worth, and A_n and C are vector coefficients. The search administrator can go far away from a reference whale by striking |A| ≥1.

$$X(t+1)=\begin{cases}\omega X^{*}(t)-A\cdot D & if\ \ p<0.5\\ D'\cdot e^{bl}\cdot\cos(2\pi l)+\omega X^{*(t)} & if\ \ p\geq 0.5\end{cases} \tag{15}$$

3.2.2. Bubble-net attacking

Whales adjust their locations by simulating hovering behavior during the upgrade, in the context of the best pursue expert's back and forth movement. The best up-and-comer course of action procured so far, target is considered a victim, and other interested executives are trying to improve the situation to a better game plan. This strategy is implemented by subtracting the simple estimator and subjective vector from the [-an, a] range specified in (16). Torque Increase Level: The torque position is used to reconstruct the spindle structure of the humpback whale (17).

$$\vec{D}=|\vec{C}.\omega\vec{X}^{*}(t)-\vec{X}(t)| \tag{16}$$

$$\vec{X}(t+1)=\omega\vec{X}^{*}(t)-\vec{A}.\vec{D} \tag{17}$$

where t is the current iteration, and is the vector of coefficients, and is the vector of position. The location vector of the best solution that has been found thus far is (21). If a better option exists, the value of X is adjusted after each iteration. Eqs. 20 and 21 are used to calculate the coefficient vectors :

$$\vec{A}=2\vec{a}.\vec{r}-\vec{a} \tag{18}$$

$$\vec{C}=2.r \tag{19}$$

r is a random vector that changes between [0, 1], and vector $\vec{a}$ declines linearly from 2 to 0 throughout the duration of iterations. In IWOA, there's a 50/50 chance that search specialists will choose either the all-encompassing method or the winding path via an irregular variable p.

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

Algorithm 1 **Improved Whale Search**

1. Create the initial community Y_j (j = 1, 2, ..., NP)
2. Calculate the capability for each discrete in Xi
3. Best discrete is X*
4. while The stopping model isn't fulfilled do
5. for every person, map the wellness to the quantity of species
6. for $j = 1 \rightarrow NP$ do
7. Choose static arbitrary $r1 \neq r2 \neq r3 \neq j$
8. Modernize $A=2a.r.a$, $a=2\text{-}t.(2/t_{max})$, $C=2.r$
9. When $i = 1$ to n do
10. Whether $p \leq \lambda$ next
11. $j == j_{rand}$ or if $rndrealj\ [0, 1) \leq CR$ then
12. else
13. Choose a arbitrary discrete X_{rand}
14. $D = |C.X_{rand} - X_i|$
15. end for

3.2.3. Attacking of Prey

The ambush behavior is seen in relation to the air pocket net assaulting idea. To display the air pockets net direct of humpback whales, two significant approaches are used. The two strategies are a winding restoring position structure and an encasing instrument. Humpback whales can use either of these two systems to catch their prey, and along these lines, the entire piece has a 50% chance of occurring. The variable p is shown as an erratic variable that shifts between [0, 1]. In Eq.20, the estimation of an is reduced when contracting with an instrument. The estimation of A can't avoid being an optional inspiration between [-a_n, a] where a is decreased from two to zero over the immovable number of cycles. The estimation of A_n is between [-1, 1] and right now |A | < 1, by then abuse is instigated and all the pursuit specialists combine to get the best strategy. The strengthening model can be given by Eq.20.

$$X(t+1) = \begin{cases} \omega X^*(t) - A \cdot D & if \quad p < 0.5 \\ D' \cdot e^{bl} \cdot \cos(2\pi l) + \omega X^{*(t)} & if \quad p \geq 0.5 \end{cases} \tag{20}$$

where p is a random number in [0,1]. In addition to the bubble-net method, the humpback whales search for prey randomly.

Interbreeding between WOA's administrators and DE's change administrator to build WOA's investigation abuse contract is at the heart of our implemented strategy Improved Whale Optimization Algorithm (IWOA). IWOA's principal administrator is a half-and-half administrator who combines DE's changes and WOA's parts, particularly enclosing prey,

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

scanning for ask, and winding refreshing location. The inquiry portion of IWOA is divided into two parts. As per Algorithm 1, if rand < λ the investigation part changes the people. λ is balanced by Eq. (21)

$$\lambda = 1 - \frac{t}{t_{\max}} \tag{21}$$

where t represent age of t_{max} providing the greatest digits of ages. We register λ to command the investigation and the misuse capacity of Improved Whale Optimization Algorithm(IWOA).
The investigation domain necessitates a shift in DE's behavior and a desire for WOA requests. Because of its prominence in researching the pursuit space, IWOA incorporates DE's change. Misuse of a section of IWOA is similar to WOA. In contrast to WOA, IWOA is a spoof detection approach. The fitter position between parent X_i and children U_i is the new location for i^{th} individual in the bleeding edge. It is vital to remember that arrangements should consider limit constraints. Eq 22 will be applied for the fixing standard if these requirements are broken.

$$X_i(j) = \begin{Bmatrix} \delta_j + rndreal\ (0,1) \times (\mu_j - \delta_j)\ if\ X_i(j) < \delta_j \\ \mu_j - rndreal\ (0,1) \times (\mu_j - \delta_j)\ if\ X_i(j) < \mu_j \end{Bmatrix} \tag{22}$$

3.3. Feature Fusion using ORBF

The optimal rule based fusion (ORBF) is used to acquire the alluring qualities from composite web administrations for further ideal determination of administration structure set in composite organizer. The standard hunt swarm searcher calculations are proposed from Ant state Optimization.

3.3.1. Optimization technique

Graph Searching Technique is used to find the shortest path from source to the objective centers. Comparably this is drawn from ants that all things considered get together and finish tasks as a gathering. An underground creepy crawly examines a type of sustenance and as it researches, it drops in a type of manufactured substances named pheromones in its manner. Along these lines, various ants can consider the kind of way using the starting at now dropped pheromones. Exactly when a creepy crawly shows up at a center point, it leaves in manufactured inventions in the entire course it has sought after. Each underground creepy crawly seeks after a relative methodology. At the point when the underground bug shows up at the center point, the degree with which the bug drops in engineered mixes is genuinely relating to the uprightness of the way.

Pheromones allow you to enter data on the way to the ant. All underground creeps treat both variables as mobile bids and attributes. In general, the quality of the derivative depends on how much you focus. This is a kind of heuristic that causes ground damage to the target. The features measure the suitability of pheromones. This is the measure of well-being, which is the amount of pheromone that ants leave at all ages and choose how unusual the old ant style is. The probability of moving from the edge of the crawl net to the edge is equal to the sum and improvement of the property.

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

Algorithm 2 Optimal rule based fusion method

```
Initialize the base attractiveness, τ, and traits, η, for each edge;

for i < Iteration Max do:

    for each ant do:

        Choose probabilistically (based on previous equation) the next state to move into;
        add that move to the tabu list for each ant;

        repeat until each ant completed a solution;

    end;

    for each ant that completed a solution do:

        Update attractiveness τ for each edge that the ant traversed;

    end;

    if(local best solutions better that global solution)

        save local best solution as global solution;

    end;

    end;
```

Burden adjusting can be accomplished adequately particularly with regards to adjusting cloud based powerful applications. A proposed improvement on subterranean insect settlement calculation has been played out that gives profoundly proficient burden adjusting to web administrations. By expanding or limiting various parameters of execution like preparing load, memory accessible, defer or arrange load for the billows of various sizes, one can build up a powerful burden balancer utilizing insect state enhancement calculation.

4. RESULTS AND DISCUSSION

This section explains the results obtained on three unquestionable databases to attest the appropriateness of proposed OFSD technique. The evaluation is done through benchmark databases - Replay-Attack, CASIA-FA and OULU-NPU databases. The redirection is finished with the going with structure: Windows 10 undertaking variation working framework, Matlab 2015a, 64G memory, two Intel E-52620 v3 CPUs and one NVIDIA GeForce GTX 1080 Ti GPU contraption.

4.1. Dataset descriptions

At the present time, given the short delineation of replay-attack/ambush, CASIA face threatening to mocking, and OULU-NPU database. These three face-deriding databases contain different kinds of real face pictures and face mocking attack pictures. The short portrayals of each database are presented as underneath.

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

4.1.1. REPLAY-ATTACK Dataset

The Replay-Attack data set contains 1300 video cuts in two ramp positions (limited level and resistance level). More than 50 users can access your account with the MacBook's webcam system, 320 × 240, Canon PowerShot camera and incredibly high quality iPhone 3GS camera. For example, three types of attacks can be displayed chronologically using printed images, images, re-published images, and certified form photos. Phone attack and tablet attacks are the most viable attacks in replay attacks where iPhone screen is used for phone attack and iPad screen is used for tablet attack. Figure 3 shows the true and false faces of the database.

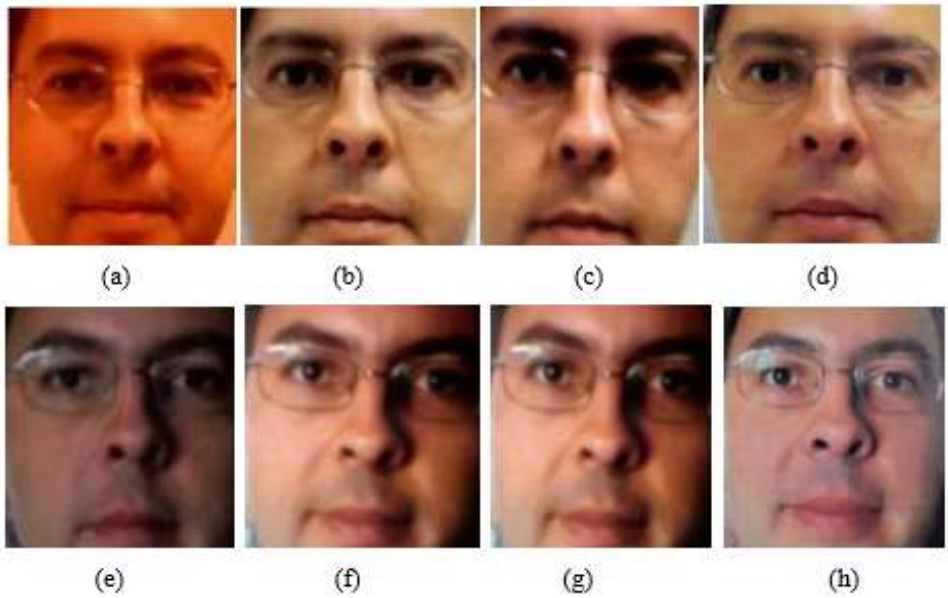

Figure 3. *Test Replay-Attack dataset image (a) controlled scenario with real image (b) controlled scenario with printed photo attack (c) controlled scenario with displayed image attack (d) controlled scenario with video-replay attack (e) adverse scenario with real image (f) adverse scenario with printed photo attack (g) adverse scenario with displayed image attack (h) adverse scenario with video-replay attack*

4.1.2. CASIA face anti-spoofing Dataset

Cassia-FA (Cassia Face-Spoofing Database) has more than 600 video clips, and 50 customers are looking for certification and ambush. Due to the ambiguous capture device, there are 3 imaging advantages to attack. For example, there are ambushes: cropping photos, playing video and improperly designed photo attacks. After the violent attack, the coordinator's eyes in the eye area appear through the eyehole: The attacker displays the real person's account on the iPad and uses the camera system to restore the chronic condition. Fig. 4 shows the cases of certifiable and fake faces in replay-attack database.

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

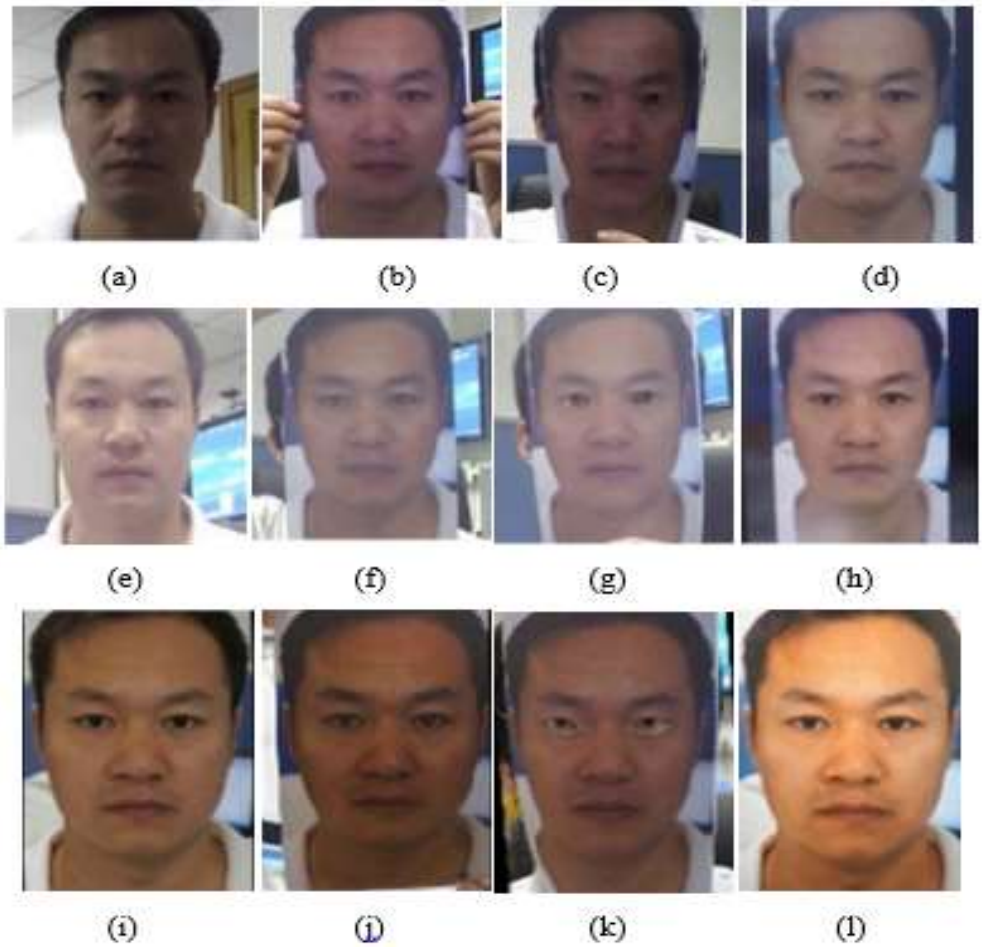

Figure 4. *Test CASIA-FA dataset (a) low quality real face image (b) low quality image with warped photo attack (c) low quality image with cut photo attack (d) low quality image with video-replay attack (e) medium quality real face image (f) medium quality image with warped photo attack (g) medium quality image with cut photo attack (h) medium quality image with video-replay attack (i) Low quality real face image (j) Low quality image with warped photo attack (k) Low quality image with cut photo attack (l) Low quality image with video-replay attack*

4.1.3. OULU-NPU database

OULU-NPU face introduction assault database includes 4950 authentic access and snare accounts that were recorded utilizing forward looking cameras of six changed PDAs. Those photographs recorded utilizing the front cameras of six PDAs in three social affairs with various light conditions and foundation scenes. The genuine finds a decent pace are obtained by 55 subjects that are separated into three subsets (20 clients) for preparing, progress (15 clients) and testing (20 clients).

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

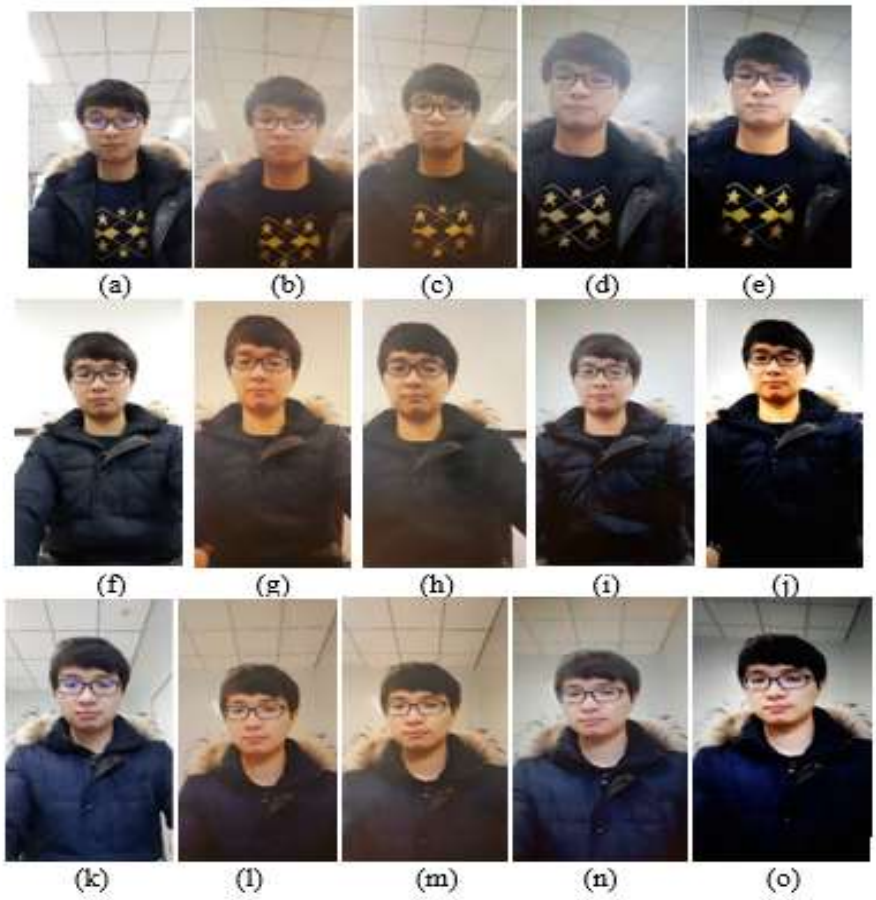

Figure 5.*Test OULU-NPU dataset (a) session-1 real-face image (b) session-1 printer-1 attack image (c) session-1 printer-2 attack image (d) session-1 dispaly-1 attack image (e) session-1 dispaly-2 attack image (f) session-2 real-face image (g) session-2 printer-1 attack image (h) session-2 printer-2 attack image (i) session-2 dispaly-1 attack image (j) session-2 dispaly-2 attack image (k) session-3 real-face image (l) session-3 printer-1 attack image (m) session-3 printer-2 attack image (n) session-3 dispaly-1 attack image (o) session-3 dispaly-2 attack image*

4.2. Evaluation metrics

EER (equivalent error rate) is the point at which the receiver operating characteristic (ROC) curve f_y rate. To get half of the total error rate (HTER), you must first find the EER points to get a range that matches the EER points in your development set. Thereafter, the HDR calculated in the test set provides the corresponding HDR to the range provided by the development package. HTER explains:

$$HTER=\frac{F_x+F_y}{2} \tag{23}$$

4.2.1. Time and memory analysis

The performance of our proposed OFSD technique is analyzed by two different metrics is time and memory. The same training data, training settings, and loss function as the LBP network are used. Generally, the input image size, network depth decides the speed of the technique. Table 1 illustrates the time and memory comparison of proposed OFSD and existing LBP techniques. From table, we observe our proposed OFSD technique needs 71MB memory during training stage, which is 21.3% efficient than

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

existing LBP technique. Moreover, OFSD technique is faster than the existing LBP technique in their training stage. Figs. 5-7 show the loss curves for three databases Replay-Attack, CASIA-FA and OULU-NPU respectively of proposed OFSD and existing LBP techniques.

Table 1 .*Time and memory comparison*

Techniques	Training		Testing	
	Time (s/epoch)	Memory (MB/images)	Time (s/epoch)	Memory (MB/images)
LBP	838.76	122	0.03	87
OFSD	721.06	98	0.015	71

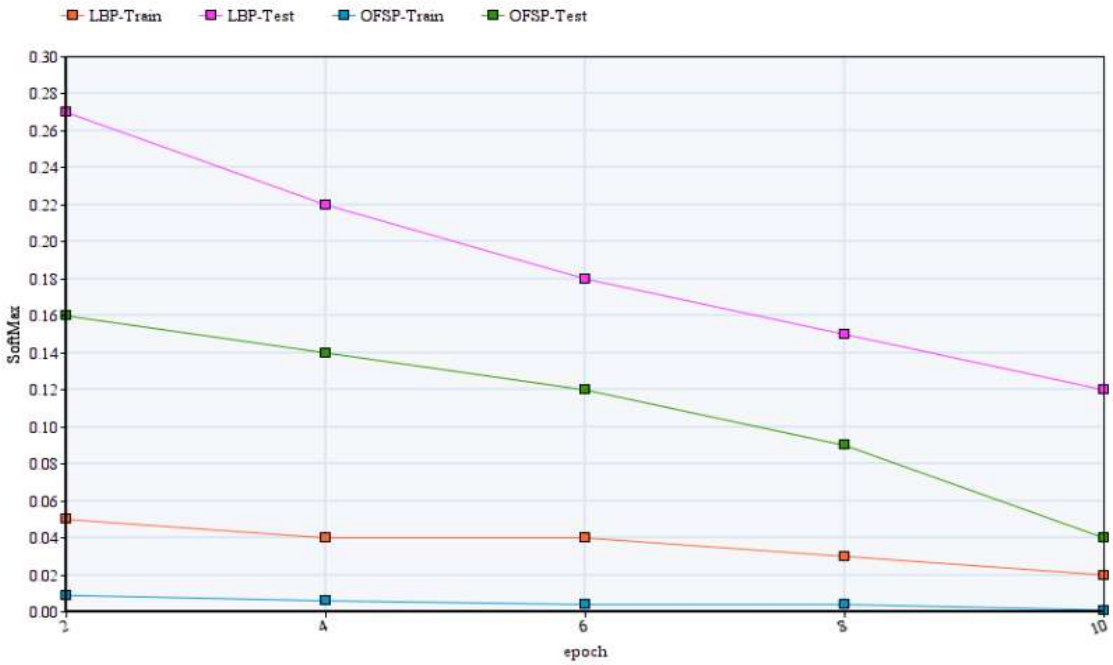

Figure. 5. *Loss curve of proposed and existing technique on Replay-Attack database*

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

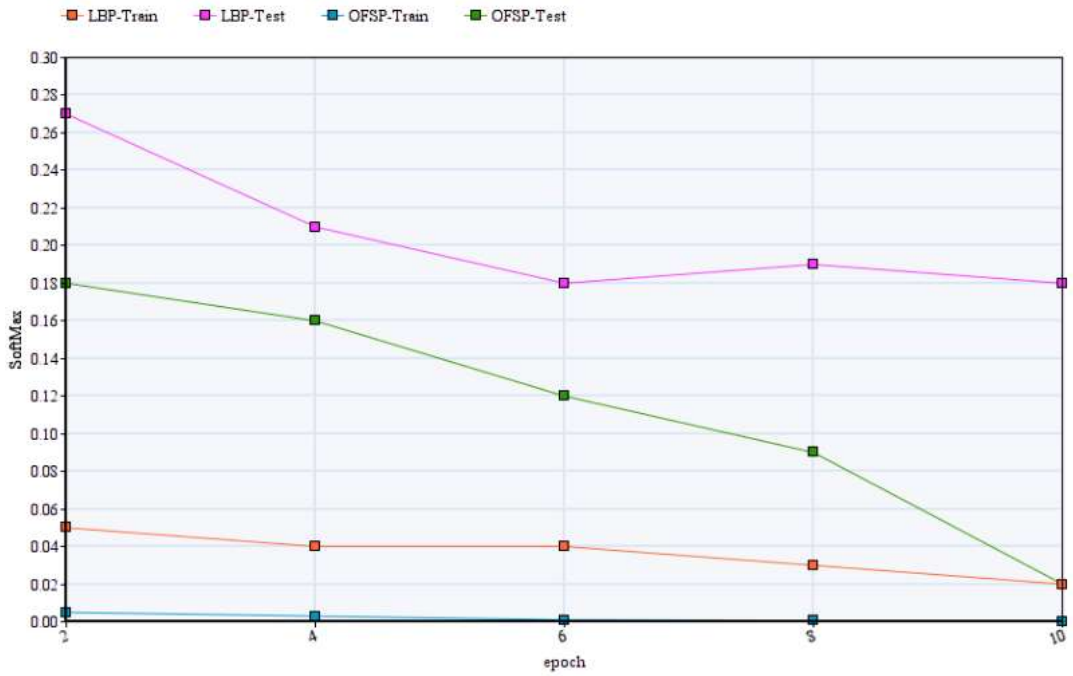

Figure. 6.*Loss curve of proposed and existing technique on CASIA-FA*

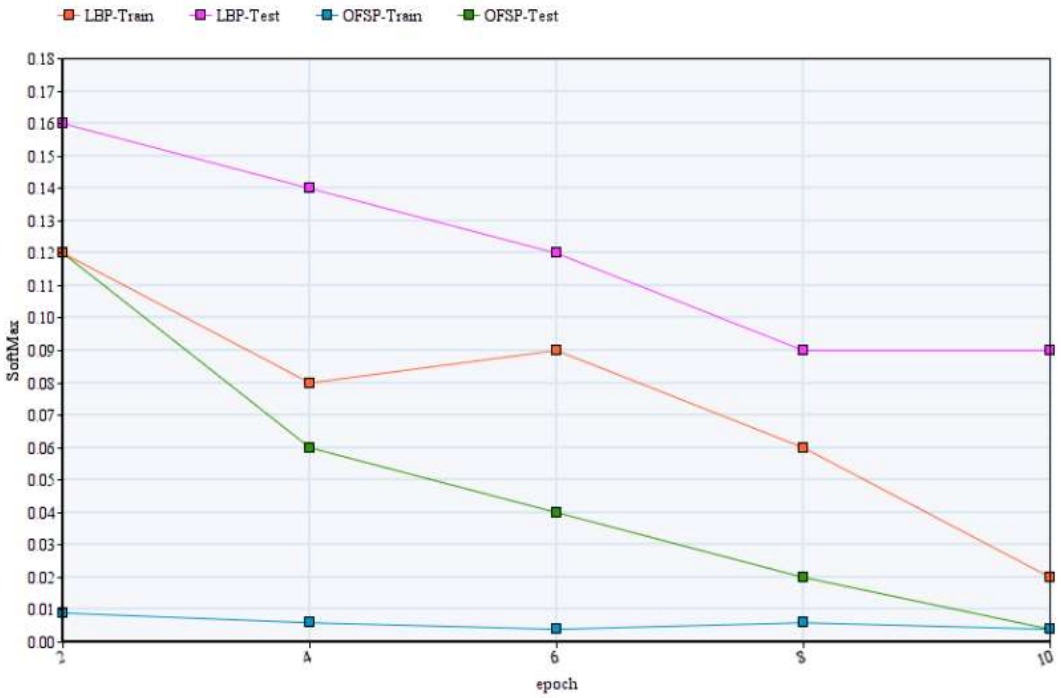

Figure. 7 .*Loss curve of proposed and existing technique on OULU-NPU*

4.2.2. Performance comparisons with state-of-the-art

To validate the prospective OFSD technique, the results are correlated with the most recent technique used to detect face fraud in Table 2. In general, the proposed OFSD technology outperforms other technologies, which shows the effectiveness of the proposed technology. For a re-attack database, the finest EER for this method is 0.6%, 0.51% is a very close match. However, HDR reduced relative HDR from 1.3% to

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

1.02%. The proposed OFSD technology provides an excellent EER in relation to the Cas Xian-FA database and describes the performance of the proposed technology. Similarly, for the OLU-NPU database, the highest EER for LBP is 5.49%, which is close to 4.31%.

Table 2

Performance comparison of proposed and existing techniques

Techniques	Replay attack		CASIA-FA attack	OLU-NPU
	EER (%)	HTER (%)	EER (%)	EER (%)
Color LBP	0.9	4.9	7.1	-
Scale LBP	0.7	3.1	4.2	-
Deep CNN	6.1	2.1	7.3	-
Partial CNN	2.9	4.3	4.5	-
LSTM CNN	-	-	5.2	-
LBP	0.6	1.3	2.5	5.49
OFSD	0.51	1.02	1.9	4.31

5. Conclusion

The research paper proposed an anti-domain attack against the DS-CNN based face recognition system. First, it shows that attacks against anti-fraud face recognition systems are more difficult and more challenging compared to other use cases involving physical attacks. Since we used the strategy of training the fake and real face dataset separately, it is easy and efficient for the system to classify the image between real and fake when an input image is given. The flexibility of the neural layers is the main reason for the better performance in detecting the spoofed images. We have demonstrated that such an attack is possible by carefully designing and modeling the distortion caused by the rebroadcast process. It is possible to capture the corrupt image and use the successfully designed test results for counterfeit detection, face detection testing and authentication methods (identifying that the victim's face is in the hands of the attacker). The main reason for presenting fake images is the flexibility of the neural layer.

REFERENCES

1. Kollreider, K., Fronthaler, H., Faraj, M.I. and Bigun, J., 2007. Real-time face detection and motion analysis with application in “liveness” assessment. IEEE Transactions on Information Forensics and Security, 2(3), pp.548-558.
2. Määttä, J., Hadid, A. and Pietikäinen, M., 2012. Face spoofing detection from single images using texture and local shape analysis. IET biometrics, 1(1), pp.3-10.
3. Raghavendra, R., Raja, K.B. and Busch, C., 2015. Presentation attack detection for face recognition using light field camera. IEEE Transactions on Image Processing, 24(3), pp.1060-1075.
4. Wen, D., Han, H. and Jain, A.K., 2015. Face spoof detection with image distortion analysis. IEEE Transactions on Information Forensics and Security, 10(4), pp.746-761.
5. Faseela, T. and Jayasree, M., 2016. Spoof face recognition in video using KSVM. Procedia Technology, 24, pp.1285-1291.
6. Feng, L., Po, L.M., Li, Y., Xu, X., Yuan, F., Cheung, T.C.H. and Cheung, K.W., 2016. Integration of image quality and motion cues for face anti-spoofing: A neural network approach. Journal of Visual Communication and Image Representation, 38, pp.451-460.
7. Wild, P., Radu, P., Chen, L. and Ferryman, J., 2016. Robust multimodal face and fingerprint fusion in the presence of spoofing attacks. Pattern Recognition, 50, pp.17-25.

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

8. Fernandes, S.L. and Bala, G.J., 2016. Developing a novel technique for face liveness detection. Procedia Computer Science, 78(C), pp.241-247.
9. Pinto, A., Pedrini, H., Schwartz, W.R. and Rocha, A., 2015. Face spoofing detection through visual codebooks of spectral temporal cubes. IEEE Transactions on Image Processing, 24(12), pp.4726-4740.
10. Villan, A.F., Candas, J.L.C., Fernandez, R.U. and Tejedor, R.C., 2016. Face recognition and spoofing detection system adapted to visually-impaired people. IEEE Latin America Transactions, 14(2), pp.913-921.
11. Boulkenafet, Z., Komulainen, J. and Hadid, A., 2016. Face spoofing detection using colour texture analysis. IEEE Transactions on Information Forensics and Security, 11(8), pp.1818-1830.
12. Patel, K., Han, H. and Jain, A.K., 2016. Secure face unlock: Spoof detection on smartphones. IEEE transactions on information forensics and security, 11(10), pp.2268-2283.
13. Yu, H., Tan, Z.H., Zhang, Y., Ma, Z. and Guo, J., 2017. DNN filter bank cepstral coefficients for spoofing detection. Ieee Access, 5, pp.4779-4787.
14. Singh, M. and Arora, A.S., 2017. A robust anti-spoofing technique for face liveness detection with morphological operations. Optik, 139, pp.347-354.
15. Wang, Y., Nian, F., Li, T., Meng, Z. and Wang, K., 2017. Robust face anti-spoofing with depth information. Journal of Visual Communication and Image Representation, 49, pp.332-337.
16. Farmanbar, M. and Toygar, Ö., 2017. Spoof detection on face and palmprint biometrics. Signal, Image and Video Processing, 11(7), pp.1253-1260.
17. Alotaibi, A. and Mahmood, A., 2017. Deep face liveness detection based on nonlinear diffusion using convolution neural network. Signal, Image and Video Processing, 11(4), pp.713-720.
18. Xia, Z., Lv, R., Zhu, Y., Ji, P., Sun, H. and Shi, Y.Q., 2017. Fingerprint liveness detection using gradient-based texture features. Signal, Image and Video Processing, 11(2), pp.381-388.
19. Cho, M. and Jeong, Y., 2017. Face recognition performance comparison between fake faces and live faces. Soft Computing, 21(12), pp.3429-3437.
20. De Souza, G.B., da Silva Santos, D.F., Pires, R.G., Marana, A.N. and Papa, J.P., 2017. Deep texture features for robust face spoofing detection. IEEE Transactions on Circuits and Systems II: Express Briefs, 64(12), pp.1397-1401.
21. Chan, P.P., Liu, W., Chen, D., Yeung, D.S., Zhang, F., Wang, X. and Hsu, C.C., 2017. Face liveness detection using a flash against 2D spoofing attack. IEEE Transactions on Information Forensics and Security, 13(2), pp.521-534.
22. Zhao, X., Lin, Y. and Heikkilä, J., 2017. Dynamic texture recognition using volume local binary count patterns with an application to 2D face spoofing detection. IEEE Transactions on Multimedia, 20(3), pp.552-566.
23. Sepas-Moghaddam, A., Malhadas, L., Correia, P.L. and Pereira, F., 2017. Face spoofing detection using a light field imaging framework. IET Biometrics, 7(1), pp.39-48.
24. Edmunds, T. and Caplier, A., 2017. Face spoofing detection based on colour distortions. IET Biometrics, 7(1), pp.27-38.
25. Li, H., He, P., Wang, S., Rocha, A., Jiang, X. and Kot, A.C., 2018. Learning generalized deep feature representation for face anti-spoofing. IEEE Transactions on Information Forensics and Security, 13(10), pp.2639-2652.
26. Zhang, L.B., Peng, F., Qin, L. and Long, M., 2018. Face spoofing detection based on color texture Markov feature and support vector machine recursive feature elimination. Journal of Visual Communication and Image Representation, 51, pp.56-69.

ISSN:2153-182X, E-ISSN: 2153-1838
Vol. 17 No. 02 (2023)

27. Rehman, Y.A.U., Po, L.M. and Liu, M., 2018. LiveNet: Improving features generalization for face liveness detection using convolution neural networks. Expert Systems with Applications, 108, pp.159-169.
28. Beham, M.P. and Roomi, S.M.M., 2018. Anti-spoofing enabled face recognition based on aggregated local weighted gradient orientation. Signal, Image and Video Processing, 12(3), pp.531-538.
29. Kavitha, P. and Vijaya, K., 2018. Optimal feature-level fusion and layered k-support vector machine for spoofing face detection. Multimedia Tools and Applications, 77(20), pp.26509-26543.
30. Rehman, Y.A.U., Po, L.M. and Liu, M., 2020. SLNet: Stereo face liveness detection via dynamic disparity-maps and convolutional neural network. Expert Systems with Applications, 142, p.113002.
31. Li, L., Feng, X., Xia, Z., Jiang, X. and Hadid, A., 2018. Face spoofing detection with local binary pattern network. Journal of visual communication and image representation, 54, pp.182-192.