applied sciences

MDPI

Review

A Comprehensive Review of Face Morph Generation and Detection of Fraudulent Identities

Muhammad Hamza [1], Samabia Tehsin [1,*], Mamoona Humayun [2,*], Maram Fahaad Almufareh [2] and Majed Alfayad [2]

[1] Department of Computer Science, Bahria University, Shangrilla Road, Sector E-8, Islamabad 44220, Pakistan
[2] Department of Information Systems, College of Computer and Information Sciences, Jouf University, Sakaka 72388, Saudi Arabia
* Correspondence: stehseen.buic@bahria.edu.pk (S.T.); mahumayun@ju.edu.sa (M.H.)

Abstract: A robust facial recognition system that has soundness and completeness is essential for authorized control access to lawful resources. Due to the availability of modern image manipulation technology, the current facial recognition systems are vulnerable to different biometric attacks. Image morphing attack is one of these attacks. This paper compares and analyzes state-of-the-art morphing attack detection (MAD) methods. The performance of different MAD methods is also compared on a wide range of source image databases. Moreover, it also describes the morph image generation techniques along with the limitations, strengths, and drawbacks of each morphing technique. Results are investigated and compared with in-depth analysis providing insight into the vulnerabilities of existing systems. This paper provides vital information that is essential for building a next generation morph attack detection system.

Keywords: face morphing; biometric forensics; morphed identities; biometrics; face recognition

Citation: Hamza, M.; Tehsin, S.; Humayun, M.; Almufareh, M.F.; Alfayad, M. A Comprehensive Review of Face Morph Generation and Detection of Fraudulent Identities. *Appl. Sci.* **2022**, *12*, 12545. https://doi.org/10.3390/app122412545

Academic Editors: Julian Fierrez and Gian Luca Marcialis

Received: 29 October 2022
Accepted: 6 December 2022
Published: 7 December 2022

1. Introduction

Life in the current era of the digital world is facilitated by many comforts. Laborious manual tasks are becoming automated with the advancement of technology. Traveling becomes a pleasure with technically advanced policies and procedures. More and more people are traveling every year by different means. People travel for studies, jobs, business, and tourism. Nowadays, most traveling procedures are automated. Nevertheless, digital systems for border control are also very common [1]. These systems are deployed in about 180 airports around the globe [2]. These systems authenticate facial identities through digital systems. The system matches the traveler's live photo identity with machine-readable travel documents (MRTD), such as a passport [1,3]. Live captured face identity must match with the approved travel document identity; otherwise, permission to enter that territory is denied. Digital systems visibly improve this process to facilitate frequent traveling requirements, and such systems are developed to speed up and facilitate a massive touring populace.

Technology has massively simplified many procedures. But it also comes with some ill usage. Many evil minds are using this technology for fraudulent activities. No technology solution is without a loophole that can be exploited. A few people are exploiting digital systems to get unauthorized entry into restricted territories. Face morphing attacks are used to fool such face recognition systems.

Image morphing techniques have been used from the 1980s to today [4]. But advancement in technology not only supports legal procedures but can also benefit unlawful activities. Technology is accessible to everyone, and photo morphing tools can be used to alter human face images.

Face morphing technology works by integrating multiple faces into a single face. Such morphing results in resembling all of the input faces. Technically, it has features of all

the contributing faces. Consequently, the morphed image can trick the automated border control system to get illegal authorization. Therefore, the face identification procedure endorses the machine-readable travel document as the captured still of the passenger matches the accomplice's passport. This technique tricks the automated system and does the human inspection. Figure 1 shows the face morphing results of two subjects. The resultant image resembles both the contributing subjects.

Moreover, the proportion of the contribution of an image can vary in the morphing process. This results in increasing the detection challenge. Therefore, image morphing can be used by any criminal on the exit control list. That person can use an abettor's morphed image identity and positively obtain travel authorization in an unlicensed state or territory.

Various research studies are presented in the literature to reduce this possibility of fraudulent identity. These methods can be grouped based on the methodology acquired. A single-morph attack detection method inspects only the morph image for traces of morph, and the differential morph detection method compares both the query-saved image and the live photo of the traveler [5].

This study focuses on reviewing the latest available morph attack detection techniques. Detailed comparison between different techniques will be done. Source databases will be analyzed and compared with respect to quality, variation, and morphing tools used. This research provides a comprehensive review of existing morph creation and detection techniques. It also analyzes the limitations of the existing work. This work can be used by other researchers to see in-depth progress of the field so far. Presented research analyzes the current and previous work on morph generation, creation, and detection. It also gives direction for future research prospects.

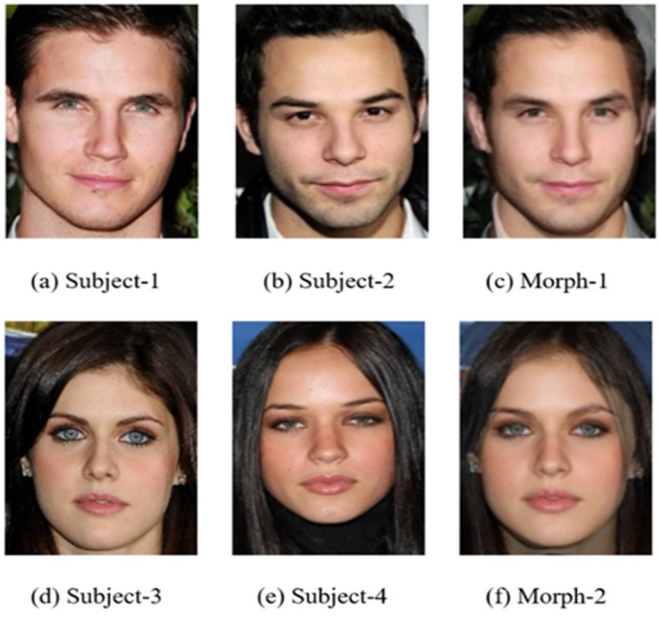

Figure 1. Morph-1 (**c**) is a morphed image created from Subject-1 (**a**) and Subject-2 (**b**). Morph-2 (**f**) is a morphed image created from Subject-3 (**d**) and Subject-4 (**e**). (Morphed images are created manually using the tool FotoMorph (2014) and Celebrity Database [6] Adapted from Chen et al. (2015).

The manuscript's significant contributions are:

I. This research explains and analyzes different morph generation techniques, tools, and their limitations.
II. It presents data repositories used for morph attack detection and their challenges and limitations.
III. It shows the evaluation metrics used as standard practice in the field.
IV. It also gives in-depth knowledge and analysis of morph detection techniques and their results on different datasets.

V. It also gives the open challenges and future research prospects of the field.

The structure of the article is as follows. Section 2 describes the source databases in detail. It also presents the evaluation metrics of the domain. State-of-the-art image morphing and morph attack detection (MAD) methodologies are also described and discussed in Section 2. Section 3 details a comparative analysis of different morph attack detection techniques that have been accomplished. The mentioned section also adds analysis, limitations, and constraints of these studies. Section 4 delivers future directions and also concludes the review of morphing attacks.

2. Materials and Methods

Face morphing attacks can result in acute consequences like terrorist activities. It has been reported that such attacks successfully tricked the border control system to get illegal authorizations. Therefore, this problem has gained considerable attention from the research community in the past few years. Various methods have been introduced in the recent past to detect face-morphing attacks. Data play a crucial role in research these days. Many face recognition databases are collected and publicly available for research purposes. However, publicly available morphing attack datasets are very limited.

2.1. Image Morphing

Earlier in the 1980s and 1990s, image morphing was employed to establish graphical effects in animated movies and entertainment videos [4]. Two or more faces are required to create the image morphs. First, spatial correlation between the two subjects is established. Then warping and intensity interpolation is used to create the morphs. Thus the resultant image is a combination of two underlying subjects and therefore resembles both. Transition control parameters are used to produce different quality outputs. These controls include warping and interpolation parameters. Many methodologies are used in the literature for image morphing. The list includes mesh warping [7], field morphing [8], and radial basis morphing. Control points are determined through the mesh grid of face landmarks. The input subject is transformed into the resultant face by freezing a few points of the face while warping the rest of the face image. Field morphing uses a corresponding set of lines to correlate the subjects. Distinct elements in the illustrations were plotted and established by calculating the distance from the specified line.

The radial basis function (RBF) morphing technique also employs the mesh of points or curves. These points or curves are established by correlating face images. After that, mapping is performed through these points and patches. FantaMorph is a professional tool used to create such morphs. Figure 2 illustrates the intermediary and final results of morphing using the specified tool.

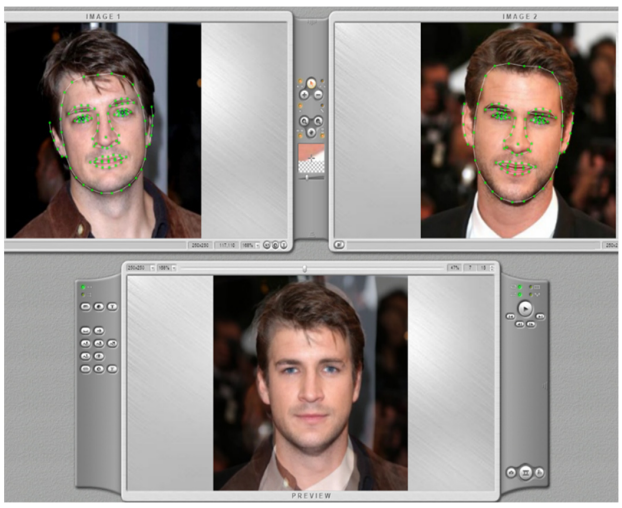

Figure 2. Morphed image created by merging two subjects in the tool FantaMorph (Version-5).

In the recent past, a lot of work has been done on generative adversarial networks (GANs). These methods are also employed for face morphing generation [9,10]. These morphs are highly dependent upon the properties of GAN used for generation. Moreover, it can pose a serious threat to morph detection if the GAN is new or unknown. Depending upon these factors, these deep learning-based morphs can be very challenging for face recognition systems.

2.2. Source Databases

Many datasets are presented in the literature for biometrics and face recognition [11–19]. For the training and testing of morph attack detection models, the databases shown in Table 1 are used. These databases are used to create morphed images utilized in morph attack detection research studies. It can be seen that different databases have a diverse range of image variations. High image variation is better for creating a generalized morph attack detection model. The number of subjects also facilitates training a generalized and robust model.

Table 1. Details about source databases and morph attack detection methodologies.

Datasets	Publication Year	No. of Images	No. of Subjects	Images Per Subject	Feature Distinction	Research Work Reference	Morphing Tools
FRGCv2	2005	28,021	4003	7	Illumination, expression, 3D	[5]	UBO Morpher [2], FaceMorpher (2018), OpenCV [18], FaceFusion (2012).
						[2]	GIMP Software (2017), Sqirlz Morph (2017).
FERET	1998	14,126	1199	Variable	Grayscale and colored lighting, a variety of facial expressions and postures, subjects of variant races, facial hair and hair style	[5]	UBO Morpher, FaceMorpher (2018), OpenCV [18], FaceFusion (2012).
						[2]	GIMP Software (2017), Sqirlz Morph (2017).
						[20]	Triangle warp, Beier-Neely field morphing method [8], and Fotomorph (2014).
FM-DB (Custom Made)	2019	1449	63	23	Expression, occlusion, make-up, gender	[1]	Customized morphing process. (Script-Code based)
AR Face Database [13]	1998	4000	126	Variable	Eyewear, scarf, expression, illumination, gender	[2]	GIMP Software (2017), Sqirlz Morph (2017).
FRAV-ABC	2020	2340	1170	2	Age, gender	[21]	GIMP Software (2017), Sqirlz Morph (2017).
BU-4DFE [14]	2008	60,600	101	600	Expression, race, gender	[20]	Triangle warp, Beier-Neely field morphing method [8], and Fotomorph (2014).
CFD [15]	2015	597	597	1	Race, gender	[20]	Triangle warp, Beier-Neely field morphing method [8], and Fotomorph (2014).
FEI (Faculty of Industrial Engineering) [22]	2015	2800	200	14	Different poses, facial expression variety, illumination change, eyewear, and varying races	[20]	Triangle warp, Beier-Neely field morphing method [8], and Fotomorph (2014).
PUT [16]	2008	9971	100	Variable	Posture, high resolution	[20]	Triangle warp, Beier-Neely field morphing method [8], and Fotomorph (2014).
						[23]	OpenCV [24]
SC-Face [17]	2011	4160	130	Variable	Quality, illumination, gender, distance, posture	[20]	Triangle warp, Beier-Neely field morphing method [8], and Fotomorph (2014).
Utrecht (Hancock, 2008)	2008	131	69	Variable	Expression, gender, race	[20]	Triangle warp, Beier-Neely field morphing method [8], and Fotomorph (2014).
Custom Made Database (All morphed)	2016	450	110	Variable	Race, gender	[23]	GIMP Software (2017)
Custom Made (morphed included)	2017	783	104	Variable	Race, gender	[22]	GIMP Software (2017)
Custom Made from FRGC and private dataset. (Morphed Included)	2020	11,293	747	Variable	Illumination, expression	[23]	OpenCV [24]

Table 1. *Cont.*

Datasets	Publication Year	No. of Images	No. of Subjects	Images Per Subject	Feature Distinction	Research Work Reference	Morphing Tools
AMSL [25]	2018	6592	52	variable	Gender	[26]	OpenCV, FaceMorpher, StyleGAN 2, WebMorpher
SOTAMD [27]	2020	5748 morphed images	150	Variable	Gender, ethnicity	[28]	FaceMorpher, FaceFusion, FaceMorph, FantaMorph, Triangulation with STASM_landmark

Similarly, the total number of images in a respective database also plays a vital role in model training and testing. Different morphing tools are used for the creation of morphed images. The quality of created morphed images varies with the utilized tool. Some tools automatically generate morphed images from original source images through a program script code, while others require manual interference to create morphed images. The studies that have utilized large databases with high variation and a variety of morphing tools depict a more realistic morph attack detection scenario.

2.3. Evaluation Metrics

Different evaluation metrics are reported in the literature for measuring the performance of morph detection systems. The evaluation metric may lead to ignoring a few important aspects and emphasizing the rest. DEER (detection equal error rate), *APCER* (attack presentation classification error rate), *BPCER* (bonafide presentation classification error rate), and *ACER* (average classification error rate) are the most commonly used metrics for this problem domain.

APCER can be defined as the percentage of morphing attacks predicted as bonafide. Mathematically,

$$APCER = 1 - \left(\frac{1}{|MA|}\right) \sum_{w=1}^{|MA|} R_w$$

here $|MA|$ is the total number of morph attacks and R_w has a value equal to one if an attack is classified correctly as an attack, zero otherwise.

BPCER can be expressed as the percentage of legitimate occurrences erroneously predicted as morph attacks.

$$BPCER = \frac{\sum_{w=1}^{|BF|} R_w}{|BF|}$$

Here $|BF|$ is the total occurrences of bonafide samples. R_w is one for bonafide image marked as bonafide, and zero otherwise.

ACER is the mean of both the quantities mentioned above.

$$ACER = \frac{APCER + BPCER}{2}$$

DEER is the detection trade-off curve point where *APCER* and *BPCER* are equal.

2.4. Methods of Morph Attack Detection

Morphed images can be detected using various methods based on the available data and computation capability. Morph attack detection (MAD) methodologies can be divided into two major categories.

- Single Image MAD Method

Single image MAD methods only rely on the morphed image for analysis and classify the input image as bonafide or morphed. It exploits the fact that morphing an image leaves some traces and artifacts. These traces are used for the detection of morphing. Texture analysis, like binary statistical image features (BSIF) [19], can be very helpful in finding these artifacts. Moreover, deep learning is also a very useful tool for detecting such morphs.

But such methods require a reliable supply of data to train from. The quality of data determines the quality of MAD methods.

- Differential MAD Method

The differential MAD method requires two images to process. One is the query image, and the other is the traveler's live image. Both images take part in the analysis and detection of morphing. Feature vectors of both specified images are obtained for assessment [1,12–17]. Demorphing is the process of identifying the accomplice. Demorphing can also be possible with the two above-mentioned images. Accomplice image can be retrieved by subtracting the query image and the live photo.

The differential morph attack detection method is extensively utilized in different studies for morph attack detection. The following techniques are prevalent in literature.

2.4.1. Image Demorphing

In image demorphing methodology, both captured images and potential morphed images are used to uncover the true identity of the owner of the document. The demorphing model performs mathematical transformations on the potentially morphed and still live images to perform its task.

The process of demorphing states that the captured image of the traveler can be linked to the potentially morphed image on the travel document and processing can be done to reveal the true identity of the authentic owner of the travel document. The process of demorphing involves the inversion of the morphing process. This approach proposes that the basic concept of morphed images is assumed to be a linear combination of the accomplice's (authentic owner of travel documents) and the criminal's images, where a criminal's image is the captured picture at the border control and the accomplice's image is the image of the person used to create a morph image by combining it with the criminal's image. The demorphed image is found by removing the live captured image from the potentially morphed image presented on the travel document. Suppose a demorphed image comparison with the live captured image produces a low score. In that case, it means that the presented image in the travel document is a morphed image instead of an authentic image of the traveller. The basic approach of a demorphing-based morph attack detection model is illustrated in Figure 3.

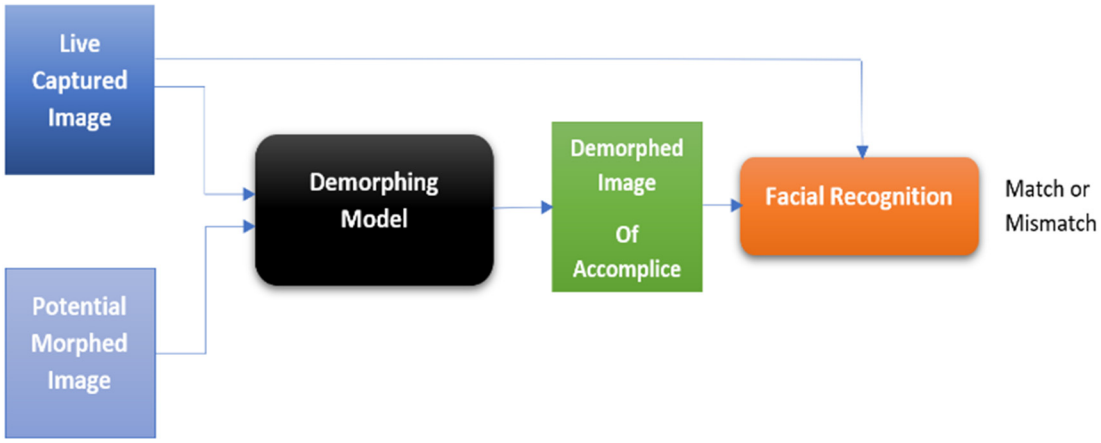

Figure 3. Basic methodology of a demorphing morph attack detection model.

FD-GAN (Face Demorphing Generative Adversarial Network for Restoring's Facial Image) was used in a previous study [1] to restore the facial image of the accomplice from a morphed image to facilitate the process of accurate morph attack detection. The FD-GAN utilizes the morphed image and the captured picture of the criminal to restore the accomplice's image. It implements the symmetric dual network architecture along with two levels of restoration losses to achieve this proposed task. Three types of images

are passed to the system for training, including the image of the criminal, the accomplice, and the morphed image. After training on these images, the FD-GAN can separate the accomplice's image from the morphed image by separating the identities of different participants in the morphed image. During the testing process, the FD-GAN takes the morphed image and the image of the criminal (live photo) to restore the image of the accomplice. Two types of losses are considered and monitored in this process. These losses are referred to as pixel-level restoration loss and feature-level restoration loss. The identity encoder is a convolution-based network that extracts the identity features from the received images. Extracted identity features are provided to the identity separation network, and the identity features of the accomplice are separated in this step. The identity features are passed through three cascaded residual facial restoration blocks to achieve complete facial restoration of the accomplice's image from the basic features. Restoration is done using up-sampling and convolution networks.

The demorphing process has also been done using a convolutional neural network-based model to detect morphing attacks. The model uses two input images: potential morph and live photos [21]. The demorphing process revealed different facial features when applied to the morphed image and the live captured still. The technique mentioned in [2,3] was used to create morphed images. Poisson image editing [29] was done to reduce the artifacts present in the morphed image and uplift the quality of the images. For verification that the traveler is the authentic owner of the passport, the image on the passport (potential morph) is compared with the live image of the traveler, and the model generates a demorphed output image. If the image on the passport is a morphed image, then the resulting demorphed output image is a new and different image from the live photo. On the contrary, if the image on the passport was not a morphed image, then the resulting demorphed output image would match the live captured picture of the traveler. Three neural networks were used in the model: two networks for two encoders and one network for the decoder. The convolutional networks performed the actual demorphing that extracted the important features from the input images and differentiated whether these extracted features were present in both images to reveal the presence of morph.

2.4.2. Feature Extraction and Comparison

In feature extraction methodology, a deep learning-based model known as the deep face model is used to extract features from the live image and potentially morphed images. A machine learning-based classifier is employed for categorizing the query images built on the extracted features.

The differential morph detection method has been used extensively in the literature by utilizing different techniques of feature extraction and comparison [1,20–25]. In [5], a robust differential morphing attack detection model was presented that efficiently classified morphed images generated from four different morphing tools. The basic methodology of a differential morph attack detection model is presented in Figure 4. During testing, the analyzed images contained unprocessed, resized, JPG2000 compressed, and print-scanned images. A pre-trained deep face recognition network was used as a feature extractor, and the proposed morph attack detection classifier was trained on the lowest layer. The deep face representation of the morphed image was expected to be different than the original image because it contained features of two images. The input images of potential morph and live pictures were pre-processed.

The pre-processed images were provided to the deep-face neural networks for feature extraction. ArcFace and Facenet neural networks were used for feature extraction. Multidimensional scaling of the difference of feature vectors was also done. The deep face representations were combined and processed by a machine learning-based classifier for training to differentiate between morphed and original images. A potential morph and a test image were provided to the model in pairs during the testing process. The neural network extracted the features from the images, and the features were combined and

forwarded to the classifier for classifying the image as original or morph. Results indicated a higher level of accuracy for MAD in comparison with the aforementioned works.

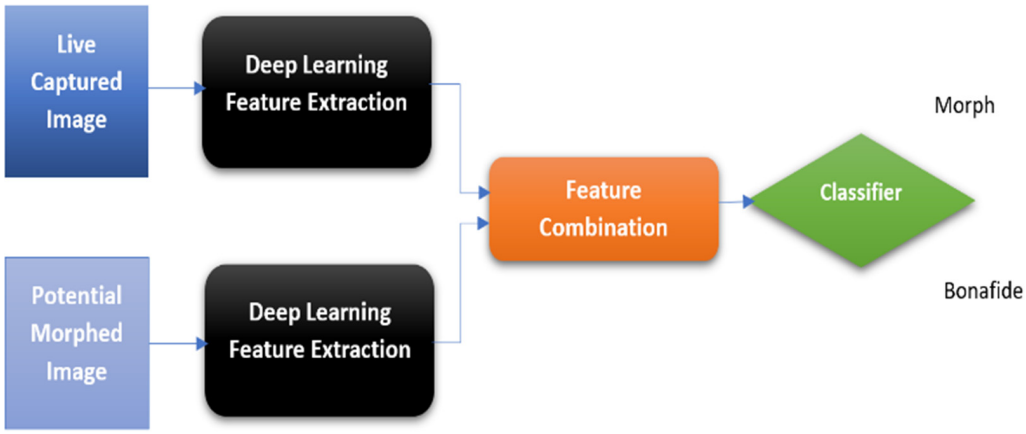

Figure 4. Basic methodology of a differential morph attack detection model.

In the study [20], an inherent vulnerability of the neural network in its learning process was highlighted, and it was proposed that this vulnerability was the root cause of their weakness against morphing attacks. Therefore, training data was introduced with different alterations to increase the robustness of the neural networks against such attacks. Layer-wise relevance propagation (LRP) of the neural networks was also analyzed to observe the variations in the decision-making process of the networks [30]. In this work, the neural network was guided to take into account the whole information of the image and to focus on specific areas for observing traces of image morphing. Two important attack scenarios were included in the study: semantic attack (normal morph attack) and adversarial attack (in which the morph creator has access to the neural network and the creator can test the system's response and manipulate its weights). A VGG19 neural network was used that contained two output neurons for classification of the original image or the morphed image. Gaussian and motion blur were used to reduce the artifacts in the morphed image to prevent the classification of these images based on these factors. Using layer-wise level propagation (LRP) [31], it was found that the neural network focused on the eye portion of images for morph detection and did not pay attention to the rest of the image. The type of information, location of information, and amount of information from images available to the neural network were controlled to force the network to consider all the information from the image to make decisions. For this purpose, partially morphed images were used in which only some portion was taken from the morphed image, and the rest of the portion of the image was from an input aligned image. Partial morphs were blended in using Poisson image editing around the eyes, nose, and mouth. The importance of the initial convolution layer was transmitted using flat-weight decomposition [32]. Overall, the robustness of the morphing attack detection model was increased in different scenarios, but a significant effect on accuracy was not observed. This study increased robustness against partial morphs from 20% to 87%.

In the domain of feature extraction, statistically independent filters were used to extract micro textures from facial morphed images. The filters were trained on natural images. The micro texture disparity was acquired using a binary statistical image feature (BSIF), and a support vector machine (SVM) based classifier classified the morphed images. Experimentation was performed on 450 morphed images, and these morphed images were created using 110 different subjects [33] (International Organization for Standardization, 2009). Feature extraction was done using a BSIF filter. The extracted features were forwarded to the SVM classifier. For this study, the trained BSIF filters were acquired from [19], and these filters were trained on 50,000 image patches [34]. Unsupervised learning was used for training the BSIF filters by utilizing the independent component analysis method [35].

The SVM classifier was trained on a set of normal face and morphed face images. VeriLook face recognition SDK (2015) was used for evaluating its performance against morphed images. According to the FRONTEX guideline rules, the false acceptance rate (FAR) was set to 0.1% (ABC, 2015). The best accuracy results (ACER—average classification error rate) were achieved in this study at 1.73%. Therefore, it is a highly suitable proposed scheme for deployment in facial recognition systems for the detection of morphed images.

In a study [27], a pre-trained convolutional neural network (CNN) was utilized for detecting morphed images even if the images were submitted digitally or in the form of a physical document. Alexnet and VGG19 were used in this study. These networks were already trained on the ImageNet database. Both networks were fine-tuned on the created database [36]. This database was created from the database in [23]. Face detection was done from the input image using the Viola–Jones technique [37]. Normalized images were fed to the neural networks of VGG19 and Alexnet in parallel. Extraction of features from the input images was done by the neural networks. Features were extracted from the FC-6 layer of the network, and then these features were converted into a vector and forwarded to the classification section. Fusion (combination) of extracted features from VGG19 and Alexnet was performed, and classification of features was done using P-CRC (probabilistic collaborative representation classifier). This classifier utilized regularized least square regression (LSR) on the learned feature vector in comparison to the test feature vector [38]. The acquired distance was utilized as a morphing score to assess the performance of the morph detector. The results of the model were significantly better than previously done work on the BSIF model. DEER (detection equal error rate) of the model was 15.5% as compared to 26.70% in the case of a print-scan test set, while there was still some difference in the case of a digital test set.

A different method was also implemented [24] that extracted features from the morph and original images in the form of residual noise. A deep multi-scale context aggregation network was implemented. This network converted the input images into denoised images, and these denoised images revealed whether the input image was a morph or a genuine facial image. The model performed denoising operations (wavelet denoise [39], block matching and 3D filtering [40], multiresolution bilateral filtering [41], and denoising convolutional neural network [42–44]) on the input images. All the denoised images were combined using aggregation, and a single denoised image was acquired by wavelet-based fusion technique (each image was decomposed into sub-bands, and the highest energy valued sub-bands from the images were combined to acquire a single denoised image). The multiscale context aggregation network (MS-CAN) of 15 layers was used based on 3×3 convolution layers that were trained on the input–output pairs that contained the image both before and after the denoising operation. MSE (mean squared error) was used within the regression to estimate the performance of the learning of the aggregation process. Residual noise was calculated as the difference between the input and denoised images (the process is repeated for bonafide and morphed images). Pre-trained Alexnet was used for feature extraction from residual noise. Residual noise was passed to the classifier (probabilistic collaborative representation classifier) for the classification process. DEER of the proposed method was significantly better, as it was lower as compared to other previously applied models for this specific issue of morph attack detection.

Many other methods are also introduced in the literature that can directly or indirectly contribute to image morphing detection [45–55].

3. Results

In the recent past, the research community has proposed noteworthy methodologies for MAD. Different techniques have been used by adopting various modifications to achieve maximum accuracy using different datasets. Different tools for morph image creation have been used. Different pre-processing methods have been utilized to remove artifacts from the created morphed images.

The previous work has been summarized in Table 2 for comparison and analysis.

Few of the reported studies have shown very impressive results. But most of the reported results are derived from less challenging data. Experimental data lacks variation in lighting conditions and facial poses. Moreover, very limited data with eyewear and headgear have been added for experimentation. Facial hair can also pose morph detection issues. These issues are totally or partially missing from the reported research to date [1,2,20,21,41]. Moreover, the morphed images can be created with dynamic weight scores of different subjects [5]. Morphed images used in these studies only contain the merger of not more than two persons. Most of the research in the literature fails to deal with images having headgear or eyewear. Furthermore, very high-quality images are used for experimentation. Low quality will pose a detection problem because of noise residuals and artifacts.

Another very important problem is the usage of two-morph images only. It is very possible that the attacker might use n-morph images, with varying weight contributions. N-morph images will be more challenging to detect if n > 2. It is also assumed that simple scripts and applications like FaceMorpher, OpenCV, and FaceFusion are used for morph creations. Resultant images are easy to detect, resulting in high accuracy.

Table 2. Comparison of research work on morph attack detection.

Reference	Year of Publication	Methodology	Dataset	Results	Limitations
[2]	2018	Correlated points are used for the extraction of coconspirator's face from morphed image.	PMDB and MorphDB (Self-built)	False positive rate of biometric system reduces from 66.4% to 6.1%.	Prior knowledge of morphing technique and parameters is required to certify proper extraction of accomplice's image. It is also required to manually remove certain traces and artifacts. Moreover only two subjects are used.
[1]	2019	Abstraction of accomplice's image is performed using double network architecture. Moreover, two restoration losses are also used.	FM-database (Self-built)	Accuracy raised 49.82% to 87.5% in simple cases. For complex cases like variety of facial expression or occluded faces, accuracy enhanced from 0.4691 to 0.649.	Only Morph-2 images are employed for experiments. Limited morphing tools are used for creation of morph images.
[21]	2020	Convolutional neural network (CNN) is employed for detection of morph attack	FRAV-ABC	Very high accuracy of 98.7% is attained for morph attack detection. DEER of 0.78% to 20.7% is also reported.	Variation in illumination, facial expressions, and bearings is not created.
[5]	2020	Deep learning solution is proposed for morph detection.	MAD database (Self-built)	DEER of 1% to 7% is reported	Variety of morphed images is created using four different tools, but those tools are not the state-of-the art tools. Does not deal well with headgear, eyewear, and illumination variation.
[20]	2020	Four training methods and layer-wise propagation are used for analyzing the morphed images.	Self-built	2.8–3.1% DEER is reported for the method	Data do not includes the images with varying lighting conditions. Moreover headgear, eyewear, and facial hair variations are also not considered.
[46]	2016	Binary statistical image features (BSIF) are used for feature representation. Classification is carried out through Support Vector Machine (SVM).	Self-built	Reportedly, average classification error rate (ACER) reduced from 37.55% to 1.73%	Morphing tools used for creation of morphed images are very limited. Only morph-2 images were used.
[27]	2017	State-of-the-art deep learning models like VGG19 and Alexnet are used for transfer learning. For classification, P-CRC is used.	Self-built	DEER decreases from 26.7% to 15.05%.	Data do not includes images with varying lighting conditions. Moreover headgear, eyewear, and facial hair variations are also not considered. Morphing tools used for creation of morphed images are very limited. Only morph-2 images are employed.
[24]	2020	Residual noise is detected using deep architecture. P-CRC classifier is used for the classification of morphed images.	Derivative of PutDB and FRGC	DEER of 2.6–8% is achieved. Comparison with previous studies is also reported, showing their DEER value between 3.83–42.2%. Computational cost also enhanced four times.	Image data having front-facing pose, static facial expression, and constant radiance used only. Only morph-2 images are employed.

It is observed that most of the research work in the literature is tested on self-built data. It led to vague comparisons between different techniques. The morphs generated with such tools leave behind artifacts and residues that can be traced with a visual inspection, so they are very easy to detect by computer systems. Consequently, these systems are hardly ever used by convicts, therefore not portraying real-world circumstances. Techniques assessed on the datasets may produce elevated detection accuracy. However, due to the aforementioned limitations, the real scenarios will not get such outputs. Face morphs created with sophisticated tools with individual attention may lead to misclassification.

It is also assumed that most of the detection methodologies work fine with the known data. If the statistical distribution of training data varies, the detection methods fail to show good results. Deep learning models learn the training data patterns and, if the morph creation methodology changes, it will lead to low classification results.

4. Conclusions and Future Research Direction

Several approaches have been proposed previously to tackle the threat of morphing attack detection, and remarkably successful results have been achieved by employing different techniques of image processing and deep learning. Different databases have been explored, and different metrics are used for evaluation of test results. The best morph detection results were acquired in the study using deep face representations with a DEER of 1% to 7% [5]. Similarly, other works also achieved very good results with DEER of 0.78% to 20% [21] and DEER of 2.8% to 3.1% [20]. This review presented the state-of-the-art techniques of the field. A lot of work has been done in the field, but a few challenges need to be addressed in future research. An extensive data repository is very much required that can have a variety of images similar to real life scenarios. Challenging scenarios like facial hair, spectacles, make-up, variation in hair style, facial expression, and posture variation, must be included. Furthermore, age variation in the data is very limited. According to ICAO protocols about travel documents, MRTD is valid for up to ten years. But the dataset has a variance of two years only. So, the experiments must be carried out on a dataset having an age variance of at least ten years. Images with variable attributes associated with subjects' age variant, expression and pose variant, lighting conditions, gender, race, hairstyle, facial hair, head gear, and eyewear should be utilized. Generalized images should be considered to increase the effectiveness of border control checkpoints. Moreover, low quality morphing tools are used in most of the studies for morph data generation. More sophisticated tools should be used for realistic examples.

This research can also help with hotel check-ins, crime investigations, security agencies, and banks. Furthermore, different countries have different rules for picture size and other image specifications. Image quality may also vary due to the diversity of technology used for image acquisition. Therefore, the morph attack detection method should be capable of dealing with such challenges so that it may be deployed to any location having different acquisition methods, lighting, subjects, and technologies. High-quality professional morphing tools should be used to generate high-quality morphed images in order to simulate a real-world scenario during testing of the model. Therefore, if this proposed model is successfully developed and implemented, then a robust, adaptable, generalized, and accurate model will be available for deployment in any travel or security agency to simplify the process of morph attack detection, and it will certify that duplicitous actions will not go unimpeded.

It is also observed that 3-morphs are not employed for the morph detection process. The complexity of morph detection will increase if three or more subjects are used for morph creation. This can also lead to a future research track for this problem.

Author Contributions: Conceptualization, S.T.; methodology, S.T., M.H. (Mamoona Humayun) and M.H. (Muhammad Hamza); software, M.H. (Muhammad Hamza), M.A.; validation, S.T. and M.H. (Muhammad Hamza); formal analysis, M.H. (Muhammad Hamza), M.A. and S.T.; investigation, M.H. (Muhammad Hamza) and S.T.; data curation, M.H. (Muhammad Hamza); writing—original draft preparation, M.H. (Muhammad Hamza); writing—review and editing, S.T.; visualization, M.F.A. and M.A.; supervision, S.T., M.H. (Mamoona Humayun). All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable for studies not involving humans or animals.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Peng, F.; Zhang, L.B.; Long, M. FD-GAN: Face De-Morphing Generative Adversarial Network for Restoring Accomplice's Facial Image. *IEEE Access* **2019**, *7*, 75122–75131. [CrossRef]
2. Ferrara, M.; Franco, A.; Maltoni, D. Face Demorphing. *IEEE Trans. Inf. Secur.* **2018**, *13*, 1008–1017. [CrossRef]
3. Scherhag, U.; Rathgeb, C.; Merkle, J.; Breithaupt, R.; Busch, C. Face Recognition Systems Under Morphing Attacks: A Survey. *IEEE Access* **2019**, *7*, 23012–23026. [CrossRef]
4. Yip, A.W.; Sinha, P. Contribution of Color to Face Recognition. *Perception* **2002**, *31*, 995–1003. [CrossRef] [PubMed]
5. Scherhag, U.; Rathgeb, C.; Merkle, J.; Busch, C. Deep Face Representations for Differential Morphing Attack Detection. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3625–3639. [CrossRef]
6. Chen, B.C.; Chen, C.S.; Hsu, W.H. Face Recognition and Retrieval Using Cross-Age Reference Coding with Cross-Age Celebrity Dataset. *IEEE Trans. Multimed.* **2015**, *17*, 804–815. [CrossRef]
7. Smythe, D.B. *A Two-Pass Mesh Warping Algorithm for Object Transformation and Image Interpolation*; Technical Report 1030; ILM Computer Graphics Department, Lucasfilm: San Rafael, CA, USA, 1990.
8. Beier, T.; Neely, S. Feature-based image metamorphosis. In Proceedings of the SIGGRAPH'92: 19th Annual Conference on Computer Graphics and Interactive Techniques, Chicago, IL, USA, 26–31 July 1992; Volume 26, pp. 35–42.
9. Zhang, H.; Venkatesh, S.; Ramachandra, R.; Raja, K.; Damer, N.; Busch, C. Mipgan—Generating strong and high quality morphing attacks using identity prior driven gan. *IEEE Trans. Biom. Behav. Identity Sci.* **2021**, *3*, 365–383. [CrossRef]
10. Venkatesh, S.; Zhang, H.; Ramachandra, R.; Raja, K.; Damer, N.; Busch, C. Can GAN generated morphs threaten face recognition systems equally as landmark based morphs?-vulnerability and detection. In Proceedings of the IWBF 2020: 8th International Workshop on Biometrics and Forensics, Porto, Portugal, 29–30 April 2020; pp. 1–6.
11. Panetta, K.; Wan, Q.; Agaian, S.; Rajeev, S.; Kamath, S.; Rajendran, R.; Rao, S.P.; Kaszowska, A.; Taylor, H.A.; Samani, A.; et al. A Comprehensive Database for Benchmarking Imaging Systems. *IEEE Trans. Pattern Anal. Mach. Intell.* **2020**, *42*, 509–520. [CrossRef]
12. Sim, T.; Baker, S.; Bsat, M. The CMU pose, Illumination, and expression database. *IEEE Trans. Pattern Anal. Mach. Intell.* **2003**, *25*, 1615–1618.
13. Martínez, A.; Benavente, R. *The AR Face Database*; Tech. Rep. #24; University Autònoma Barcelona: Bellaterra, Spain, 1998.
14. Yin, L.; Chen, X.; Sun, Y.; Worm, T.; Reale, M. A high-resolution 3d dynamic facial expression database. In Proceedings of the 2008 8th IEEE international conference on automatic face gesture recognition, Amsterdam, The Netherlands, 17–19 September 2008; pp. 1–6. [CrossRef]
15. Ma, D.S.; Correll, J.; Wittenbrink, B. The chicago face database: A free stimulus set of faces and norming data. *Behav. Res. Methods* **2015**, *47*, 1122–1135. [CrossRef] [PubMed]
16. Kasiski, A.; Florek, A.; Schmidt, A. The PUT face database. *Image Process. Commun.* **2008**, *13*, 59–64.
17. Grgic, M.; Delac, K.; Grgic, S. Scface—Surveillance cameras face database. *Multimed. Tools Appl.* **2011**, *51*, 863–879. [CrossRef]
18. Senthilkumar, R.; Gnanamurthy, R.K. A detailed survey on 2D and 3D still face and face video databases part I. In Proceedings of the 2014 International Conference on Communication and Signal Processing, Melmaruvathur, India, 3–5 April 2014.
19. Kannala, J.; Rahtu, E. BSIF: Binarized statistical image features. In Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012), Tsukuba, Japan, 11–15 November 2012; pp. 1363–1366.
20. Seibold, C.; Samek, W.; Hilsmann, A.; Eisert, P. Accurate and robust neural networks for face morphing attack detection. *J. Inf. Secur. Appl.* **2020**, *53*, 102526. [CrossRef]
21. Ortega-Delcampo, D.; Conde, C.; Palacios-Alonso, D.; Cabello, E. Border Control Morphing Attack Detection with a Convolutional Neural Network De-Morphing Approach. *IEEE Access* **2020**, *8*, 92301–92313. [CrossRef]
22. Kussul, E.; Baydyk, T. Face recognition using special neural networks. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), Killarney, Ireland, 12–17 October 2015.

23. Raghavendra, R.; Raja, K.B.; Busch, C. Exploring the usefulness of light field cameras for biometrics: An empirical study on face and iris recognition. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 922–936. [CrossRef]
24. Venkatesh, S.; Ramachandra, R.; Raja, K.; Spreeuwers, L.; Veldhuis, R.; Busch, C. Detecting Morphing Face Attacks Using Residual Noise from Deep Multi-Scale Context Aggregation Network. In Proceedings of the IEEE Winter Conference on Applications of Computer Vision (WACV), Snowmass, CO, USA, 1–5 March 2020.
25. AMSL Face Morph Image Data Set. Available online: https://omen.cs.uni-magdeburg.de/disclaimer/index.php (accessed on 20 December 2021).
26. Sarkar, E.; Korshunov, P.; Colbois, L.; Marcel, S. Vulnerability analysis of face morphing attacks from landmarks and generative adversarial networks. *arXiv* **2020**, arXiv:2012.05344.
27. Raghavendra, R.; Raja, K.B.; Venkatesh, S.; Busch, C. Transferable deep-cnn features for detecting digital and print-scanned morphed face images. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, HI, USA, 21–26 July 2017; pp. 1822–1830.
28. Hamza, M.; Tehsin, S.; Karamti, H.; Alghamdi, N.S. Generation and Detection of Face Morphing Attacks. *IEEE Access* **2022**, *10*, 72557–72576. [CrossRef]
29. Pérez, P.; Gangnet, M.; Blake, A. Poisson image editing. In Proceedings of the SIGGRAPH '03: ACM SIGGRAPH 2003 Papers, San Diego, CA, USA, 27–31 July 2003; pp. 313–318.
30. Bach, S.; Binder, A.; Montavon, G.; Klauschen, F.; Müller, K.-R.; Samek, W. On pixel-wise explanations for non-linear classifier decisions by layer-wise relevance propagation. *PLoS ONE* **2015**, *10*, e0130140. [CrossRef]
31. Lapuschkin, S.; Binder, A.; Montavon, G.; Müller, K.-R.; Samek, W. The layer-wise relevance propagation toolbox for artificial neural networks. *J. Mach. Learn. Res.* **2016**, *17*, 1–5.
32. Samek, W.; Wiegand, T.; Müller, K.-R. Explainable artificial intelligence: Under-standing, visualizing and interpreting deep learning models. *ITU J. ICT Discov.* **2018**, *1*, 39–48.
33. Ferrara, M.; Franco, A.; Maltoni, D. The magic passport. In Proceedings of the IEEE International Joint Conference on Biometrics, Clearwater, FL, USA, 29 September–2 October 2014; pp. 1–7.
34. Hyvearinen, A.; Hurri, J.; Hoyer, P.O. *Natural Image Statistics*; Springer: Berlin/Heidelberg, Germany, 2009; Volume 39.
35. van Hateren, J.H.; van der Schaaf, A. Independent component filters of natural images compared with simple cells in primary visual cortex. *Proc. R. Soc. London. Ser. B Biol. Sci.* **1998**, *265*, 359–366. [CrossRef] [PubMed]
36. Scherhag, U.; Raghavendra, R.; Raja, K.; Gomez-Barrero, M.; Rathgeb, C.; Busch, C. On the vulnerability of face recognition systems towards morphed face attack. In Proceedings of the 5th International Workshop on Biometrics and Forensics (IWBF 2017), Coventry, UK, 4–5 April 2017; pp. 1–6.
37. Viola, P.; Jones, M.J. Robust real-time face detection. *Int. J. Comput. Vis.* **2004**, *57*, 137–154. [CrossRef]
38. Cai, S.; Zhang, L.; Zuo, W.; Feng, X. A probabilistic collaborative representation-based approach for pattern classifi-cation. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, 27–30 June 2016.
39. Donoho, D.L. De-noising by soft-thresholding. *IEEE Trans. Inf. Theory* **1995**, *41*, 613–627. [CrossRef]
40. Dabov, K.; Foi, A.; Katkovnik, V.; Egiazarian, K. Image denoising by sparse 3-d transform-domain collaborative fil-tering. *IEEE Trans. Image Process.* **2007**, *16*, 2080–2095. [CrossRef] [PubMed]
41. Zhang, M.; Gunturk, B.K. Multiresolution bilateral filtering for image denoising. *IEEE Trans. Image Process.* **2008**, *17*, 2324–2333. [CrossRef] [PubMed]
42. Zhang, K.; Zuo, W.; Chen, Y.; Meng, D.; Zhang, L. Beyond a gaussian denoiser: Residual learning of deep CNN for image denoising. *IEEE Trans. Image Process.* **2016**, *26*, 3142–3155. [CrossRef] [PubMed]
43. Zhang, N.; Deng, W. Fine-grained LFW database. In Proceedings of the International Conference on Biometrics (ICB), Halmstad, Sweden, 13–16 June 2016.
44. Qin, L.; Peng, F.; Ventatesh, S.; Ramachandra, R.; Long, M.; Busch, C. Low Visual Distortion and Robust Morphing Attacks Based on Partial Face Image Manipulation. *IEEE Trans. Biom. Behav. Identity Sci.* **2021**, *3*, 72–88. [CrossRef]
45. Georghiades, A.; Belhumeur, P.; Kriegman, D. From few to many: Illumination cone models for face recognition under variable lighting and pose. *IEEE Trans. Pattern Anal. Mach. Intell.* **2001**, *23*, 643–660. [CrossRef]
46. Raghavendra, R.; Raja, K.B.; Busch, C. Detecting morphed face images. In Proceedings of the IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, USA, 6–9 September 2016; pp. 1–7.
47. Mallick, S. Face Morph Using OpenCV. 2016. Available online: www.learnopencv.com/face-morph-using-opencv-cpp-python (accessed on 10 January 2022).
48. Wolberg, G. Image Morphing: A Survey. *Vis. Comput.* **1998**, *14*, 360–372. [CrossRef]
49. Gross, R.; Mathews, I.; Cohn, J.; Kanade, T.; Baker, S. Multi-PIE. In Proceedings of the 8th IEEE International Conference of Automatic Face and Gesture Recognition, Amsterdam, The Netherlands, 17–19 September 2008.
50. Atallah, R.R.; Kamsin, A.; Ismail, M.A.; Abdelrahman, S.A.; Zerdoumi, S. Face Recognition and Age Estimation Implications of Changes in Facial Features: A Critical Review Study. *IEEE Accesss* **2018**, *6*, 28290–28304. [CrossRef]
51. Raja, K.; Ferrara, M.; Franco, A.; Spreeuwers, L.; Batskos, I.; de Wit, F.F.; Gomez-Barrero, M.; Scherhag, U.; Fischer, D.; Venkatesh, S.; et al. Morphing Attack Detection—Database, Evaluation Platform and Benchmarking. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 4336–4351. [CrossRef]

52. Hong, D.; Yao, J.; Meng, D.; Xu, Z.; Chanussot, J. Multimodal GANs: Toward Crossmodal Hyperspectral–Multispectral Image Segmentation. *IEEE Trans. Geosci. Remote Sens.* **2021**, *59*, 5103–5113. [CrossRef]
53. Hong, D.; Gao, L.; Yokoya, N.; Yao, J.; Chanussot, J.; Du, Q.; Zhang, B. More Diverse Means Better: Multimodal Deep Learning Meets Remote-Sensing Imagery Classification. *IEEE Trans. Geosci. Remote Sens.* **2021**, *59*, 4340–4354. [CrossRef]
54. Raja, K.; Gupta, G.; Venkatesh, S.; Ramachandra, R.; Busch, C. Towards generalized morphing attack detection by learning residuals. *Image Vis. Comput.* **2022**, *126*, 104535. [CrossRef]
55. Bhoj, N.; Bhadoria, R.S. Time-Series based Prediction for Energy Consumption of Smart Home Data Using Hybrid Convolution-Recurrent Neural Network. *Telemat. Inform.* **2022**, *75*, 101907. [CrossRef]