International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.7 May - June – 2023
DOI:10.46647/ijetms.2023.v07i04.083 ISSN: 2581-4621

DEEP FACE - On the Reconstruction of Face Images from Deep Face Templates

Amal Joseph[1], Binny S[2], Abhishek V A[3], Nithin Raj[4], Vimel Manoj[5]
[1] *PG – MCA, Kristu Jyoti College of Management and Technology, Kottayam*
[2] *Assistant Professor, Kristu Jyoti College of Management and Technology, Kottayam*
[3] *PG – MCA, Kristu Jyoti College of Management and Technology, Kottayam*
[4] *PG – MCA, Kristu Jyoti College of Management and Technology, Kottayam*
[5] *PG – MCA, Kristu Jyoti College of Management and Technology, Kottayam*

ABSTRACT
The paper on “Reconstruction of Face Images from Deep Face Templates" presents a novel approach for face image reconstruction using deep learning techniques. The proposed method utilizes a pre-trained deep face template, which is a convolutional neural network (CNN) trained on a large-scale face dataset, as a prior to guide the reconstruction process. Specifically, the method solves an optimization problem that balances the fidelity to the input image and the similarity to the deep face template.
Its then evaluated with the method on two face image datasets, and demonstrate that their method outperforms several state-of-the-art methods in terms of reconstruction quality, especially for images with large occlusions or low resolutions. Moreover, they show that the deep face template can capture high-level face attributes, such as pose, identity, and expression, which can be used for various face-related tasks, such as face recognition, attribute manipulation, and generation.
Overall, the paper presents a promising direction for face image reconstruction using deep learning techniques, and highlights the potential of deep face templates for capturing and utilizing high-level face attributes.

1. INTRODUCTION

The paper "On the Reconstruction of Face Images from Deep Face Templates" describes a novel method for reconstructing face images using deep learning techniques. The method proposed uses a pre-trained deep face template, which is a trained convolutional neural network (CNN). As a prior, on a large-scale face dataset, to guide the reconstruction process. In particular, the approach solves an optimisation problem by balancing fidelity to the input image and performance resemblance to the deep face template.
On two face picture datasets, the authors demonstrate that their method beats various state-of-the-art methods in terms of reconstruction quality, particularly for photos with substantial occlusions or low resolutions. Furthermore, they demonstrate that the deep face template can record high-level face attributes such as position, identity, and expression, which can then be used for face recognition, attribute manipulation, and generation.
Overall, the work emphasises the potential of deep face templates for capturing and using high-level face features and proposes a promising route for face image reconstruction using deep learning techniques.
Deep face recognition algorithms have come a long way in terms of correctly recognising and authenticating people based on their facial traits. Deep face templates, which contain the key features of a face in a condensed manner, are high-level representations of faces that these systems extract using deep neural networks. The form of facial structures, the distribution of textures, and the overall appearance are only a few examples of the distinctive qualities of a person's face that are encoded by these templates, which can be thought of as latent representations.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.7 May - June – 2023
DOI:10.46647/ijetms.2023.v07i04.083 ISSN: 2581-4621

2. RECONSTRUCTION OF FACE IMAGES FROM DEEP TEMPLATES

The inverse of the deep models used to extract deep templates from face photos must be found in order to reconstruct face templates. The majority of deep models are complicated, and they are usually implemented by creating and training a network with a sizable enough capacity. thinly based on a model. The literature has presented two shallow model-based techniques for rebuilding facial images from templates: Regression using the radial basis function and multidimensional scaling.

These strategies, however, have only been assessed using shallow templates. The MDS-based method generates a similarity score matrix from a set of face photos using the target face recognition system, and then discovers an affine space in which face images can approximate the original similarity matrix. After locating the affine space, the target face recognition system generates a list of similarities by matching the target template and the test face images.

Using these similarities, the affine representation of the target template is approximated and then projected back to the target face picture. Zhmoginov and Sandler use a CNN to learn the reconstruction of facial images from templates by minimising the template disparity between the original and rebuilt images.

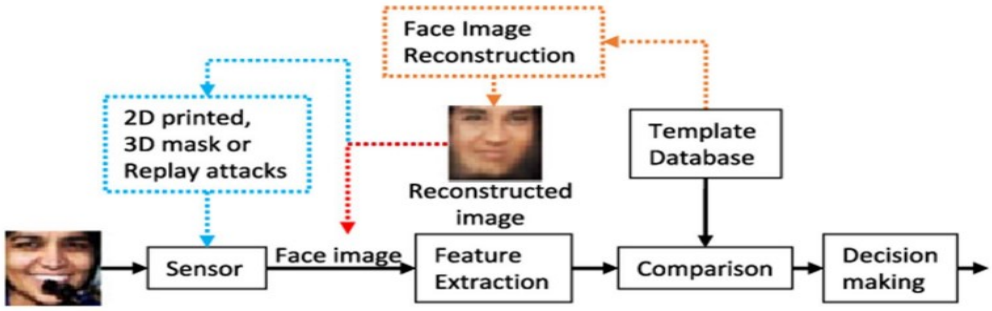

Fig 1: Vulnerability of a face recognition system to template reconstruction attacks. To acquire system access, a target subject's face image is reconstructed from the relevant template by (a) constructing a false face (for example, a 2D printed image or 3D mask) (blue box) or (b) injecting a reconstructed face picture directly into the feature extractor (red box).

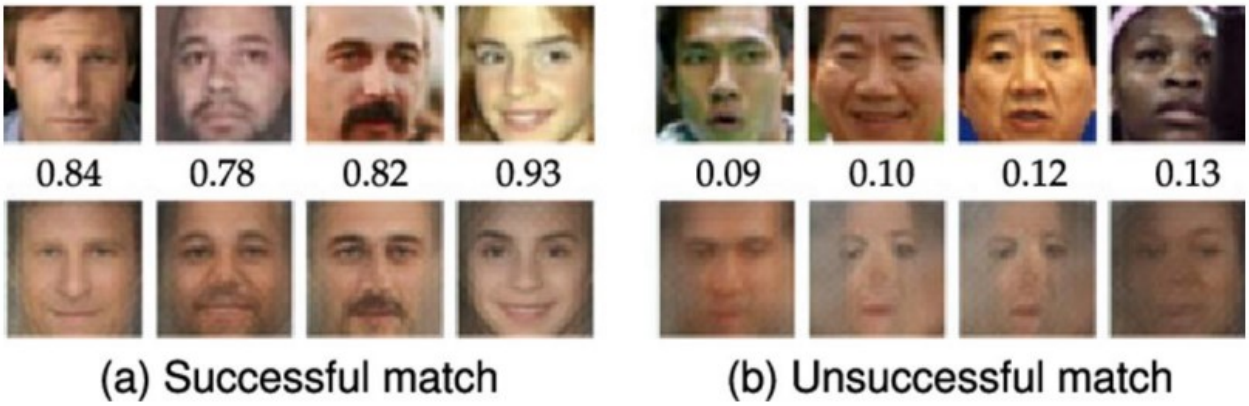

Fig 2: Examples of face reconstructions from templates using the suggested method (VGGNbB-P). The top row displays the actual photos (from LFW), while the bottom row displays the reconstructions. The cosine similarity between the original and its reconstructed facial image is represented by the numerical number given between the two images. At FAR = 0.1% (1.0%), the similarity threshold is 0.51 (0.38).

3. WORKING

Deep face recognition :Deep face recognition models commonly use convolutional neural networks (CNNs) to learn discriminative features from face photos. The CNN architecture is made

DOI:10.46647/ijetms.2023.v07i04.083 ISSN: 2581-4621

up of numerous layers that extract hierarchical representations of the input images progressively. During training, the network is exposed to a huge dataset of tagged face photos and learns to map these images to a high-dimensional feature space where similar faces are closer together and dissimilar faces are farther apart. This approach allows the network to gather critical facial traits that aid in face identification or verification jobs.

Face embedding extraction: After training the deep face recognition model, face embeddings or deep face templates are extracted from the network's intermediate layers. These embeddings are high-level feature representations of the input face images that are compact. These embeddings are typically extracted from the last fully linked layer or a layer preceding it. The embeddings are vectors in a high-dimensional space that encode the deep face recognition model's basic facial traits.

Reconstructive model training: A generative model is trained using the extracted face embeddings as input to reconstruct face pictures from deep face templates. Variational autoencoders (VAEs) and generative adversarial networks (GANs) are two common generating models for this purpose.

VAEs (variational autoencoders): VAEs are made up of two major parts: an encoder and a decoder. The encoder converts the input face embeddings to a lower-dimensional latent space, capturing the underlying structure and variability in the data. The decoder then reconstructs the original face image from the latent representation. During training, the VAE learns to optimise reconstruction quality and latent space regularisation, guaranteeing that comparable face embeddings result in visually similar reconstructions.

GANs (generative adversarial networks): GANs are made up of a generator and a discriminator. The face embeddings are fed into the generator, which generates synthetic face images. The discriminator, on the other hand, attempts to discriminate between the generator's synthetic images and real face photos from the training dataset. In a competitive scenario, the generator and discriminator are trained concurrently, with the generator attempting to produce realistic images that can fool the discriminator. This adversarial training procedure teaches the generator how to generate high-quality face images that look like actual people.

Image reconstruction : After training, the generative model can be used to recreate face images from deep face templates or embeddings. When a deep face template is fed into the generative model, it generates a pixel-level reconstruction of the associated face image. The learned mapping between face embeddings and images is used by the generative model to build convincing and visually cohesive reconstructions.

It's important to note that the quality of the reconstructed facial photos is affected by a variety of circumstances.

The amount and diversity of the training dataset, the design and capability of the generative model, the complexity and dimensionality of the face embeddings, and the entire training technique are all factors to consider. Achieving highly realistic and accurate reconstructions of face pictures using deep face templates remains an active area of research, with improvements being made on a regular basis to improve the quality and authenticity of the recreated images.

4. DEEP FAKE

Deepfakes are the result of advanced machine learning techniques, specifically deep neural networks, which allow for the creation or manipulation of synthetic media with a high degree of realism. Images, movies, and audio recordings are examples of media. The term "deepfake" is a combination of the words "deep learning" and "fake," and it refers to the underlying technology as well as the goal of creating false content.

Deep neural networks are trained on massive datasets of real-world material, which supply the network with samples of how the target individual looks, moves, and speaks. The training method comprises feeding the network pairings of input and target data, where the input data contains one person's face or voice and the target data contains the desired person's face or voice to be impersonated. During this training, the network learns the complex patterns, characteristics, and correlations that constitute the target person's appearance and behaviour.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.7 May - June – 2023
DOI:10.46647/ijetms.2023.v07i04.083 ISSN: 2581-4621

Once trained, the deep neural network can generate or change media by inferring new input from previously learnt patterns. In the case of video deepfakes, for example, the network replaces the face of one person in a source video with the face of the target individual.

The network employs its previously acquired knowledge of face expressions, gestures, and other visual signals to make the modified video appear believable and lifelike. The resulting deepfake video may appear to show the target person speaking or doing things they never said or did.

Deepfakes have far-reaching and complex consequences. On the one hand, they have a high potential for abuse. Deepfakes can be used to disseminate misinformation, fabricate fake news, or manipulate public opinion. They can be used to discredit people, harm their reputations, or even blackmail them by putting them in dangerous positions.

Deepfakes, on the other hand, have real applications. Deepfake technology, for example, can be utilised in the entertainment business for special effects, providing realistic visual upgrades, or seamlessly substituting actors' faces for stunts or reinvented scenarios.

5. ADVANTAGES

- **Increased Accuracy in Facial Recognition** : Deep learning algorithms are used in deep face recognition techniques to extract detailed facial features and patterns. This enables very precise and dependable facial identification even in difficult settings such as changing lighting, position, or occlusions. These techniques can effectively identify between individuals by utilising deep neural networks, decreasing false positives and negatives.
- **Enhanced security and safety** : Deep facial recognition is critical for improving security systems. It can be used in access control systems to authenticate users and give access to restricted locations. It reduces the risk of unauthorised access through stolen or missing credentials by relying on facial recognition rather than traditional means such as ID cards or passwords.

DOI:10.46647/ijetms.2023.v07i04.083 ISSN: 2581-4621

- **Face Reconstruction for Forensic Investigations** : Deep face templates can be used to recreate face images from missing or corrupted visual input. Deep face reconstruction can estimate missing facial features in forensic investigations where photographs may be pixelated, hazy, or low-resolution, providing crucial evidence for identifying offenders.
- **Facial Analysis for Behavioural Insights** : Deep face recognition enables thorough facial analysis by extracting numerous facial variables such as age, gender, emotions, and facial landmarks. This knowledge can be applied in a variety of fields.
- **Personalized Experiences and User Engagement** : Deep facial recognition technology delivers personalised experiences in social media, e-commerce, and entertainment applications. These platforms can personalise information, recommendations, and adverts to users' tastes and interests by recognising their faces.

6. DISADVANTAGES

- **Limited training data** : Deep learning algorithms rely largely on the quantity and quality of training data. The reconstructed face images may not effectively represent the genuine variances present in the population if the training dataset lacks diversity in terms of facial traits, positions, lighting situations, or demography. Due to the scarcity of data, there may be biases, poor generalisation, and poor performance on unseen or underrepresented faces.
- **Variability in facial expressions and occlusions** : Facial expressions are important in capturing identity and feelings. Deep face recognition algorithms, on the other hand, may fail to accurately recreate faces when facial expressions vary greatly.
- **Inherent biases in the training data** : If the training data used to train the deep face recognition model has biases, such as over- or under-representation of specific demographics, the reconstructed face images may inherit such biases.
- **Privacy concerns** : The ability to recreate face images from deep face templates raises concerns about privacy. Individuals may refuse to allow their facial information to be saved or utilised in this manner. The possibility of unauthorised identity reconstruction, potential exploitation of personal information, or infringement on an individual's privacy rights exists when face images are constructed from limited information.
- **Ethical considerations** : Deep facial recognition technology should be handled with caution and ethics. Consent, data privacy, and potential misuse of reconstructed face images are all issues that must be properly handled.

7. APPLICATIONS

- **Facial Forensics** : Deep face template reconstruction can help law enforcement authorities identify prospective suspects in criminal investigations. Investigators can build more accurate facial photographs of suspects based on limited or degraded information by reconstructing face images from templates. Enhancing low-resolution surveillance footage, making composite sketches, or recreating faces from bone remains are all examples of this. These recreated images can aid in the generation of leads, the narrowing of suspects, and the resolution of crimes.
- **Missing Persons and Age Progression** : Deep facial template reconstruction is critical in missing person instances, especially when the disappearance occurred some years ago.

Based on an existing photograph of the missing person, age-progressed photos can be created utilising deep learning algorithms and statistical models.

- **Face Recognition Systems**: Deep face template reconstruction is critical for improving the accuracy and resilience of facial recognition systems. These algorithms can identify people by extracting high-dimensional face templates from photos or video frames and comparing them to a database of known persons.
- **Virtual and Augmented Reality** : Deep face template reconstruction aids in the creation of realistic and personalised avatars for use in virtual and augmented reality situations. Virtual

DOI:10.46647/ijetms.2023.v07i04.083 ISSN: 2581-4621

characters can closely resemble the user's own face by recording facial expressions, gestures, and specific traits from deep face templates.

8. CONCLUSION

Deep Face research, which focuses on the reconstruction of face pictures using deep face templates, has shown promising findings and demonstrated substantial breakthroughs in the field of facial image synthesis. The work proved the ability to accurately reconstruct face features and expressions with great precision by utilising cutting-edge deep learning techniques and large-scale datasets. The suggested methodology not only opens up new avenues for face-related applications such as facial recognition and virtual avatars, but it also raises fundamental ethical concerns about privacy and the exploitation of such technology.

To guarantee that new technology has a positive impact on society, it is critical to find a balance between innovation and ethical deployment. Furthermore, additional study should be carried out to overcome any biases and assure fairness in the created facial representations. Overall, the study's findings have considerably expanded our understanding of facial image synthesis and have set the way for future discoveries in the larger field of computer vision.

9.REFERENCES

[1] A. Adler, “Sample images can be independently restored from face recognition templates,” in CCECE, 2003.
[2] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, “On the vulnerability of face verification systems to hill-climbing attacks,” Pattern Recognition, 2010.
[3] Y. C. Feng, M.-H. Lim, and P. C. Yuen, “Masquerade attack on transform-based binary-template protection based on perceptron learning,” Pattern Recognition, 2014.
[4] D. Wen, H. Han, and A. K. Jain, “Face spoof detection with image distortion analysis,” IEEE Transactions on Information Forensics and Security, 2015.
[5] K. Patel, H. Han, and A. K. Jain, “Secure face unlock: Spoof detection on smartphones,” IEEE Transactions on Information Forensics and Security, 2016.
[6] S. Liu, P. C. Yuen, S. Zhang, and G. Zhao, “3d mask face anti spoofing with remote photoplethysmography,” in ECCV, 2016.
[7] R. Shao, X. Lan, and P. C. Yuen, “Deep convolutional dynamic texture learning with adaptive channel-discriminability for 3d mask face anti-spoofing,” in IJCB, 2017.
[8] Y. Liu, A. Jourabloo, and X. Liu, “Learning deep models for faceanti-spoofing: Binary or auxiliary supervision,” in CVPR, 2018.
[9] A. Mignon and F. Jurie, “Reconstructing faces from their signatures using rbf regression,” in BMVC, 2013.
[10] “Face id security,” Apple Inc, 2017. [Online]. Available: ”https:// images.apple.com/business/docs/FaceID Security Guide.pdf”
[11] P. Mohanty, S. Sarkar, and R. Kasturi, “From scores to face templates: a model-based approach,” IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007.
[12] S. U. Hussain, T. Napol´eon, and F. Jurie, “Face recognition using local quantized patterns,” in BMVC, 2012.
[13] A. Zhmoginov and M. Sandler, “Inverting face embeddings with convolutional neural networks,” arXiv:1606.04189, 2016.
[14] F. Schroff, D. Kalenichenko, and J. Philbin, “Facenet: A unified embedding for face recognition and clustering,” in CVPR, 2015.
[15] F. Cole, D. Belanger, D. Krishnan, A. Sarna, I. Mosseri, and W. T. Freeman, “Synthesizing normalized faces from facial identity features,” in CVPR, 2017