IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11674

CAPSULE-FORENSICS: USING CAPSULE NETWORKS TO DETECT FORGED IMAGES AND VIDEOS

Latha M S[1], Abdul samad[2], Alekhya B[3], Harshitha M[4], Ms Rakshitha P[5]

[1,2,3,4]Student, Department of Computer Science & Engineering, Atria Institute of Technology, Bangalore, India

[5]Assistant professor, Department of Computer science & engineering,

Atria Institute of Technology, Bangalore, India

Abstract: Attackers can now fabricate pictures and movies more easily because to advances in media production tools. A video downloaded from a social media can be used to make forgeries in real time.Although state-of-the-art Detecting fake photos and videos is a difficult task. This article use a capsule network to detect several types of spoofing attacks, ranging from replay attack employing graphics or scanned movies to deep convolutional neural network-generated bogus videos. It broadens the scope of capsule networks' use beyond their initial intent. We are working on the creation of a model that will be able to solve complex graphics problems. It will involve image datasets for training and testing.

Terms used – capsule network, computer generated video, forgery detection replay attack

1. INTRODUCTION

Fake news media can be created using forged photos and videos to go around facial authentication. With the improvement in the complex network and the utilisation of large amount of trained data, the quality of modified photos and videos has significantly improved.Facial fraud has been much easier as a result of this.

A video clip of the particular individual or an identification photo is all that is required nowadays to build a forged facial impression. The true fake issue is a prominent illustration of this threat: anyone with a computer may create films combining the facial image of any celebrity using a human image synthesis approach based on AI powered.

Other approaches, such as Fridrich and Kodovsky's method, are more adaptable, as they can be used for both solution analysis and face reenact video detection. This research uses a capsule network to identify counterfeit images and videos in a range of forging conditions, including replay detecting attacks and (including completely and partially) machine image/video detection.

2. RELATED WORK

Forgery detection is achieved via a number of approaches, many of which are two-fold (targeting both computer-generated images and videos).Below is a quick rundown of the most popular algorithms, sorted by the features and types they employ. We also go over the fundamentals of capsule networking and the dynamic routing method that enables them.

2.1. Replay Attack Detection

LBP approaches were the principal defence against replay attacks prior to the latest machine learning age. This method was introduced by Kim, which is based on the LSPs and produces more accuracy than LBP methods. With the introduction of true fake issue the capacity to detect replay and various attacks has more improved. Yang et al method's classifies features extracted by a previously trained Convolutional or deep neural network using a support vector machine.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11674

3. CAPSULE-FORENSICS

3.1. System Architecture

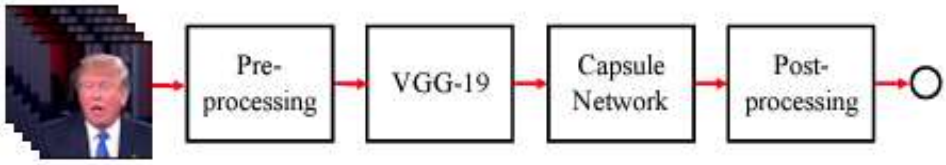


Fig. 1.Summary of proposed model.

Both photos and videos can be used with the suggested technique (Fig. 1). The data is divided into pixels during the pre-processing phase for video source. The categorization results are then obtained using the frames (posterior probabilities). In the post-processing phase, the probabilities are combined to get the final result. The left out components are constructed similarly to when the input is an image. Faces are recognised and scaled to 128 x 128 in the pre-processing step and using the component of VGG-19 network to provide input to the capsule network. To reduce the size of the input to the capsules networking, we use the result of the third max pooling instead of the three outputs before the Rectified linear layers.

3.2. Capsule Design

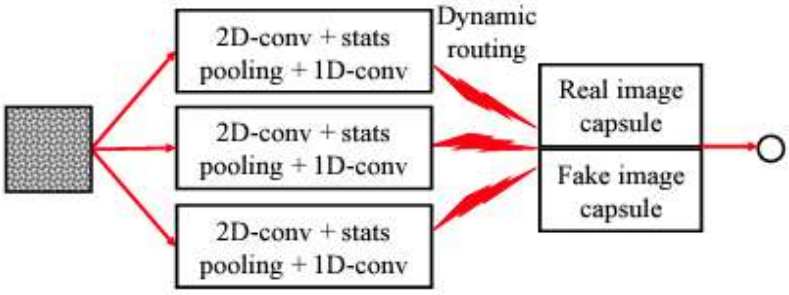


Fig. 2. Capsule architecture in broad network of forensics

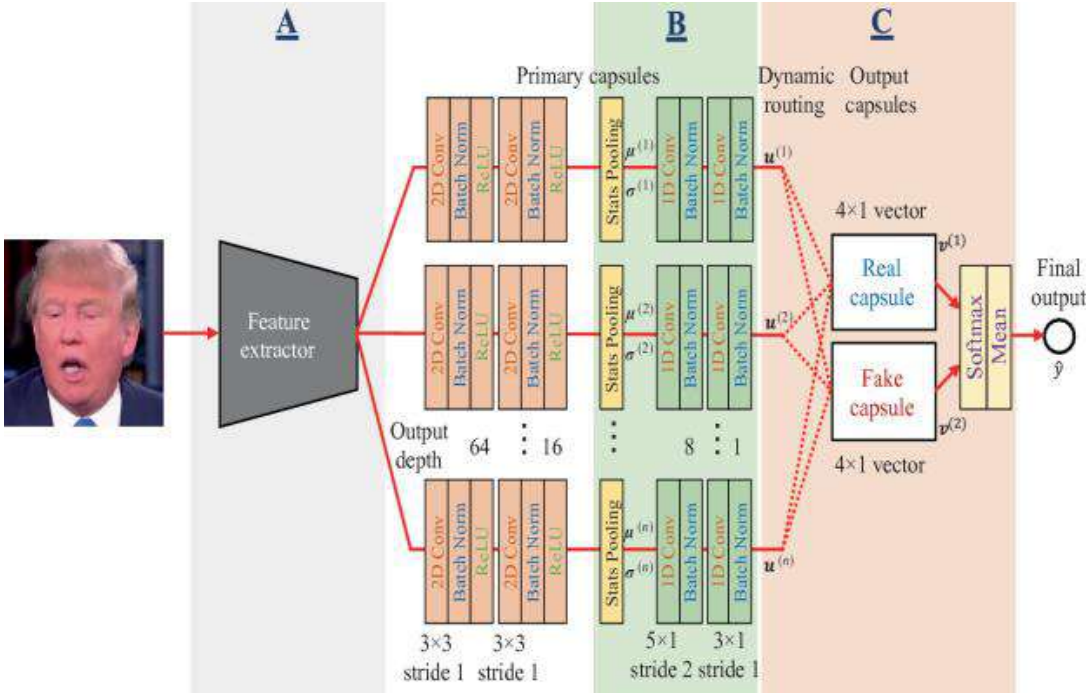


Fig 3. Capsule network architecture

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11674

A proposed network is made up of three core capsules and two discrete capsules, one for genuine images and the other for fake images. The VGG-19 network distributes the inputs to the three major capsules. Statistical pooling plays a crucial part in fraud detection, and it is used here as well, as seen in the diagram.Algorithm dynamically routes the outputs of the three capsules to the output capsules for repetitions.

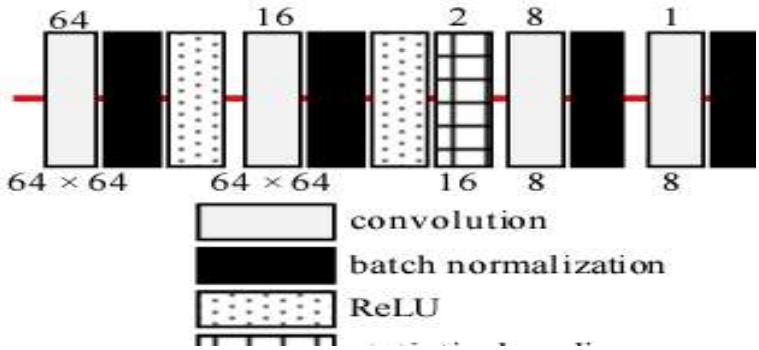


Fig 4. Complete design of primary(main) capsule.

Algorithm 1 Dynamic routing between capsules.

procedure ROUTING($\mathbf{u}_{j|i}, W, r$)
  $\hat{W} \leftarrow W + rand(size(W))$
  $\hat{\mathbf{u}}_{j|i} \leftarrow \hat{W}_i squash(\mathbf{u}_{j|i})$ ▷ $W_i \in R^{m \times n}$
  for all input capsule i and all output capsules j **do**
    $b_{ij} \leftarrow 0$
  for r iterations **do**
    for all input capsules i **do** $c_i \leftarrow softmax(b_i)$
    for all output capsules j **do** $\mathbf{s}_j \leftarrow \sum_i c_{ij} \hat{\mathbf{u}}_{j|i}$
    for all output capsules j **do** $\mathbf{v}_j \leftarrow squash(\mathbf{s}_j)$
    for all input capsules i and output capsules j **do**
      $b_{ij} \leftarrow b_{ij} + \hat{\mathbf{u}}_{j|i} \cdot \mathbf{v}_j$
  return $\mathbf{v}_j$

Before iterating the routing, we adjusted the approach by adding Gauss noisy data to the three- dimensional weight tensor and executing another compression . The extra chaos helps to prevent overfitting, while the extra formula keeps the connection steady. The graphic below depicts the results of the core and secondary capsules**.**

cross-entropy loss function:

$$\mathbf{v}_j = squash(\mathbf{s}_j) = \frac{\|\mathbf{s}_j\|^2}{1 + \|\mathbf{s}_j\|^2} \frac{\mathbf{s}_j}{\|\mathbf{s}_j\|}$$

$$L = -\left(y \log(\hat{y}) + (1 - y) \log(1 - \hat{y})\right),$$

If y denotes the regression coefficients name and y denotes the expected name, and m denotes the number of dimensions of the output.

$$\hat{y} = \frac{1}{m} \sum_i softmax \left(\begin{bmatrix} \mathbf{v}_1^\intercal \\ \mathbf{v}_2^\intercal \end{bmatrix}_{:,i} \right)$$

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11674

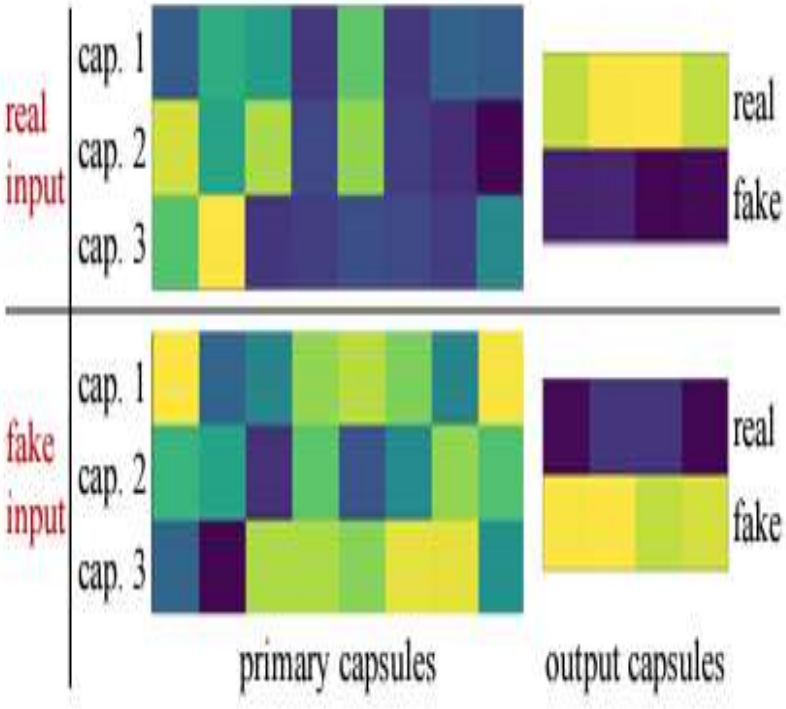


Fig 5. Representation of Real or Fake capsule

Core and secondary(output) capsules derived average results from genuine and false photos generated using the Face2Face approach. Between actual and artificial inputs, three main capsules behave dramatically differently. Despite the fact that their weights differ, there is a lot of agreement in the output capsules.

4. EVALUATION

In order to determine the benefit of employing the random noise and then we examined the experimental setup either with or without the background noisy data. The output was generated noise was using a normal distribution and was utilized for training purpose only.The dynamic routing technique employed two rounds (r = 2). The accuracy and half total error rate were employed as measurements.

4.1. Face Swapping Detection

We investigated our suggested method's ability to detect face swapping using a fake accounts strategy at both the frame and video levels . Demonstrate that in both instances, our proposed random noise method has the maximum accuracy.

4.2. Facial Reenactment Detection

Using the face-to-face approach we tested the method capacity to identify facial reenactment . For data processing, we strictly followed the authors' instructions. The performance of the proposed method (both with and without noise) was comparable to that of the best-performing state-of-the-art methods. We also placed our technique through its paces on video, comparing it to Afchar et al MesoNet .'s facial video forgery detection network . Instead of using the entire video, we merely used the first ten frames for our concept and our method has outperformed the Afchar et al.'s network.

4.3. Fully Computer-Generated Image Detection

There are multiple of state-of-the-art ways for detecting internet images or videos, including the live video methodology for face flipping, the face-2-face method for visual reenactment, and deep video evaluation portraits procedure for the intent of fraud . On digitally created photos and photographic images, we analyze our designed method with state-of-the-art methods in order to achieve the best accuracy.

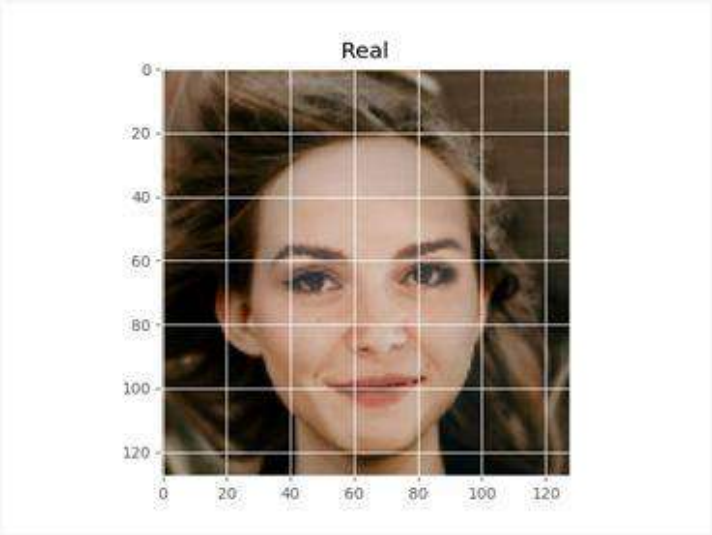
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

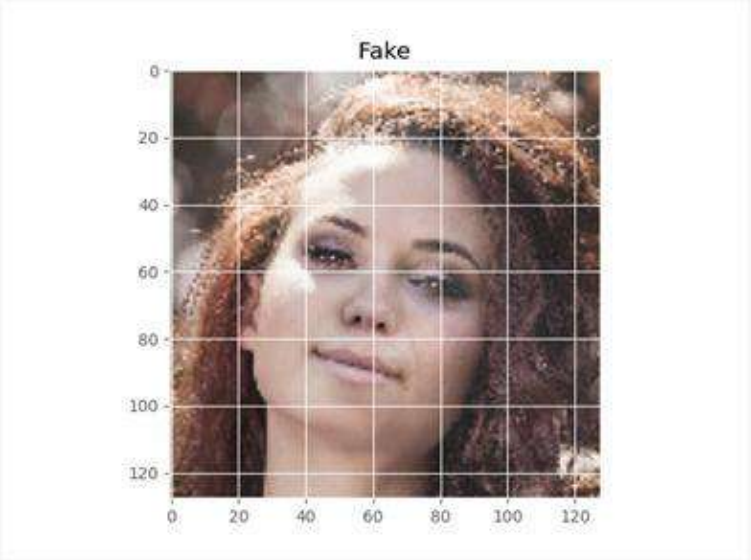
International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11674

5. RESULTS:



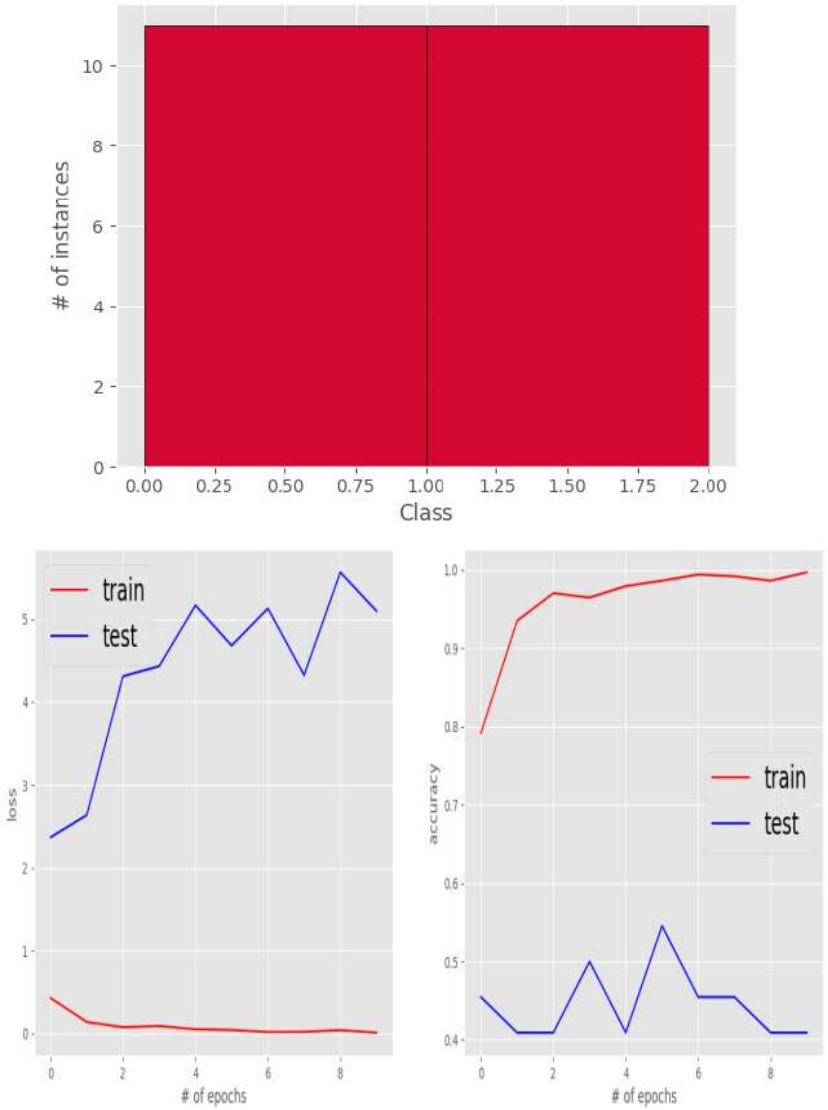


IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11674



6. CONCLUSION

The capsule network method has been used to detect the forgery pictures and videos and use of the random noise during the training phase was very advantageous and able to build a generic detection system against the forged images and videos .The purpose method to withstand against the machine techniques which are unfriendly, particularly the proposed random noise at test time, will be evaluated and improved in future study. In the future, it should more concentrate on making the suggested methods more resistant against the mixed attacks that is both the image and video attack , we need to promote the awareness on this subject among the people and researchers so this method we get more capacity against the attacks and the forgery of the images and videos will be reduced in the future.

7. REFERENCES

[1] Justus Thies, Michael Zollhofer, Marc Stamminger, Christian Theobalt, and Matthias Nießner, “Face2Face: Real-time face capture and reenactment of RGB videos,” in CVPR. IEEE, 2020.

[2] Hyeongwoo Kim, Pablo Garrido, Ayush Tewari, Weipeng Xu, Justus Thies, Matthias Nießner, Patrick Perez, Christian Richardt, Michael Zollh ´ ofer, and Chris- ¨ tian Theobalt, “Deep video portraits,” in SIGGRAPH. ACM, 2019.

[3] Hadar Averbuch-Elor, Daniel Cohen-Or, Johannes Kopf, and Michael F Cohen, “Bringing portraits to life,” ACM TOG, 2021.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11674

[4] Joon Son Chung, Amir Jamaludin, and Andrew Zisserman, "You said that?," arXiv preprint arXiv:1705.02966, 2020.
[5] SupasornSuwajanakorn, Steven M Seitz, and Ira Kemelmacher-Shlizerman, "Synthesizing obama: learning lip sync from audio," ACM TOG, 2018.
[6] "Terrifying high-tech porn: Creepy 'deepfake' videos are on the rise," https://www.foxnews.com/ tech/terrifying-high-tech-porncreepy-deepfake-videos-are-on-therise, Accessed: 2020-02-17.
[7] Ivana Chingovska, Andre Anjos, and S ´ ebastien Marcel, ´ "On the effectiveness of local binary patterns in face anti-spoofing," in BIOSIG, 2018.
[8] Tiago de Freitas Pereira, Andre Anjos, Jos ´ e Mario ´ De Martino, and Sebastien Marcel, "Can face anti- ´ spoofing countermeasures work in a real worldscenario?," in ICB. IEEE, 2019.
[9] Yuezun Li, Ming-Ching Chang, Hany Farid, and SiweiLyu, "In ictu oculi: Exposing AI generated fake face videos by detecting eye blinking," arXiv preprint arXiv:1806.02877, 2018.
[10] Jessica Fridrich and Jan Kodovsky, "Rich models for steganalysis of digital images," IEEE TIFS, 2018.