Meta-Brisque: Cost Efficient Image Spoofing Detection for Realtime Applications

Abdul Raoof Wani
AUUP Noida India
wanirauf@gmail.com

Amit Bora
CCFIS Noida India
amit@ccfis.net

Nitin Pandey
AUUP Noida India
npandeyg@gmail.com

Ajay Rana
AIIT, Amity University Uttar Pradesh
Noida, India
ajay_rana@amity.edu

***Abstract*- We always seek to change and develop new things as per our requirements and needs which is good for our survival. Our curiosity to find and discover the unknown opens the doors towards a better future. This curiosity has led us to work and learn about the new fields not only in technology (Robotics, AI, AR, VR, MR, IoT etc.) but also in other domains like Agriculture, Communication, Finance, Security etc. The security domain has seen drastic changes in the past decade from physical to information security. The latest trends in security are focused on Face Detection and Recognition (FDR) technology that has a wide variety of applications but every technology comes with its drawback and here a major threat is Spoofing. To tackle this, methods have been developed based on Neural Networks (NN) to get better results but these methods don't seem to be feasible in terms of cost. In this paper, we tried to provide a method named Meta-BRISQUE for image spoofing detection in Realtime FR applications (based on Metadata and BRISQUE) which is cost-efficient and nearly accurate as currently available solutions.**

Keywords – Image Processing; Image Metadata; Image Spoofing; CNN; BRISQUE

I. INTRODUCTION

In recent years, we have seen that FDR has shown major advancement in three areas entertainment, IoT and security. The entertainment domain does not use the complete method but only the first half of technology (Face detection). There are mobile apps (Like FaceApp) in a market that detects faces present in images and provides different filters to be applied over the detected region and transform into something else. IoT and Security domain uses FDR to detect the person and perform certain actions on recognition bases. For example, once the image is captured and FDR is performed, the authenticity of an individual is determined as per the Database (DB) of legitimate users of the device. When detected person is verified as per DB, than only access is granted to them. But like every other thing, FDR also has cons related to it. This technology is vulnerable to spoofing attacks. When someone tries to gain unauthorized access to a system/ environment by masquerading as a registered user in the presence of FDR is known as spoofing. Three widely used image spoofing attacks are print, replay and 3D masks. Print attacks are those where a person tries to fool/bypass the FDR system by showing the printed image of a registered person. Replay attacks are ones in which intruder plays a repeated video file (to avoid protocols for print attacks) of the registered person. In the third one, intruder makes a wearable 3D mask of the registered person. By altering the basic attack, sub-variants of these also have been developed and their countermeasures are also discussed in [17].

Spoof detection can be done by either Image Quality Assessment (IQA) or NN based methods. IQA determines the accuracy of the image based on two methods subjective and objective. Subjective methods are work on human perception and hard to compute whereas objective methods work on computation and prediction of image parameters like a blur, reflection, color etc. Further based on the availability of reference images objective methods are of 3 types: Full Reference (FR), Reduced Reference (RR) and No Reference (NR). FR uses a reference image similar to the test image; RR extracts features from both reference-test images and compares them; NR doesn't have any reference image and generates a score based on a computation of image parameters. Many Neural Network-based models have also been proposed by different authors that provided very good results but we think, results obtained comes with high cost. Cost in terms of hardware, resources and high amount of data to train the model. We don't always have a large amount of data to predict something and training a network with fewer data results in the undertrained network which won't be able to provide accurate results, turning time and money to waste. Similarly, Reference-based IQA methods would show decent results till the test images have similar reference images but the time some different image is placed they will also fail. Here, we are using the NR method BRISQUE for IQA. [1] BRISQUE acronym for Blind/Referenceless Image Spatial Quality Evaluator calculates the Natural scene statistics (NSS) using Mean Subtracted Contrast Normalization (MSCN) and generating pairwise relation of MSCN image to shifted image in four orientations. These Five new images are passed to Generalized Gaussian Distribution (GGD) and Asymmetric Generalized Gaussian Distribution (AGGD) to generate a 36x1 feature vector. This feature vector is passed to Support Vector Machine (SVM) to predict the score based on the trained model.

BRISQUE being trained on public dataset don't always give the accurate result. So, in order to reduce this gap, we used the Metadata of the image. In real-time applications, no one gets a chance to tamper or modify images which alters the metadata of the file, which means, we get the original metadata. Metadata is the data/ information about any data. We found that almost all images that come directly from a real-time application show different values over two parameters. So, we used these parameters to extend the BRISQUE model in cases where the score gets higher than the threshold to classify the image as normal or spoof.

Further sections of a paper are as follows: Section II discusses the related work, Section III discusses the experimentation, Section IV gives the Result and Discussions and Section V with a conclusion.

978-1-7281-7016-9/20/$31.00 ©2020 IEEE

II. RELATED WORK

[1] provided an NR model BRISQUE that generated a score in the range of 0-100 for the input image (0 being the best quality and 100 being the worst) using the pixel normalization of an image with MSCN; generating feature vector with GGD, AGGD and score prediction with SVM. Authors in [3] focused on print quality defects and provided a method to detect these defects with textures, local shape features (using LBP and Gabor wavelets), low-level feature descriptors (using HOG), classification (with SVM). [4] proposed to use two different color spaces (CIE L*u*v and YC_rC_b) to generate six normalized histograms (ranging between 0-255) corresponding to each component of color spaces. Combining the histograms together to generate a feature vector and generating the result as a spoof or not using Extra Trees Classifier (ETC). [5] provided CNN based approach where two CNN are used: Patch-based CNN (using DNN) to extract texture information with LBP in random patches and Depth based CNN (using FCN) to extract the depth map estimated by 3D face model-fitting algorithm in HSV and YC_bC_r color spaces. [6] provided face spoofing detection method based on Image Distortion Analysis (IDA). They generated feature vector of the input image from features like reflection, blur, color diversity, chromatic movement etc. trained an Ensemble classifier over different face spoof attacks and passed the feature vector to classifier for result prediction. [7] proposed to used Local Ternary Patterns (LTP) rather LBP (as the later ones are sensitive to noise and illumination) for textural feature extraction, divided them to upper and lower patterns to generate histograms and then histograms are fed to SVM for prediction. [8] worked mainly on face spoof detection in video rather than images. They used the LSTM-CNN model where LSTM is placed above the CNN layer in order to extract the temporal relationship between video frames and CNN for detection of the frame as a spoof or not. [9] did a comparative study on different Neural Network-based models like CNN, 3DCNN, CNN+LSTM, CNN + convLSTM on raw data in a single stream and in two streams (fusion method with the optical flow). [10] proposed CNN can't extract temporal features but for face spoof detection in videos Spatio-temporal features are must, so, LBP-TOP was used for extraction of Spatio-temporal feature extraction and CNN for further processing. [11] proposed fine-tuning based transfer learning on VGG-16 CNN. They used the pre-trained model and fine-tune its weights by retraining in order to get desired results for face spoof detection. [12] proposed a multi-cues based NN approach concatenating three feature maps: shearlet-based IQAF (SBIQF), motion cues driven average Optical Flow Magnitude (OFM) map and scene OFM map together and passing the previous result to a two-class SoftMax classifier. [13] proposed a face-antispoofing method based on CNN & Kinect. CNN for texture analysis and classifying it as a spoof or not with SVM and depth information collected using Kinect. The collective result of Kinect and CNN decides the final result. [14] also used transfer learning like [11] but with different CNN i.e. Deep Residual Network (ResNet-50) which provides input to LSTM (to learn local temporal features) and uses FC layer with SoftMax to get the end result. [15] proposed to use video frames with CNN to extract features so that the temporal information within frames also gets utilized and trained an SVM classifier to get the end result over publicly available datasets for validation.

Table I contains a list of datasets that are available publicly for research purposes regarding image spoofing.

TABLE I. LIST OF PUBLICLY AVAILABLE DATASET FOR FACE ANTI-SPOOFING.

S.no	Dataset
1.	Replay attack
2.	CASIA
3.	CASIA-FASD
4.	3D-MAD
5.	NUAA photo imposter
6.	MSU MFSD
7.	MSU USSD
8.	Cork Print Attack Database
9.	Yale Recaptured Database
10.	Print Attack Database
11.	LIVE IQA

III. EXPERIMENTATION

First, we obtain metadata of the image sent from a mobile device over the network. The metadata contains multiple parameters over which we require only two (exposure value and brightness value). Once, the parameters are obtained, we check the exposure value; if the value is "non-zero", then, the image is normal but if it is 0, we have to take brightness value into consideration. A "positive brightness value" represents the "spoof" image and "negative value" represents a "zoom/normal" image. Figure 1 shows the flow for classification as per metadata parameters.

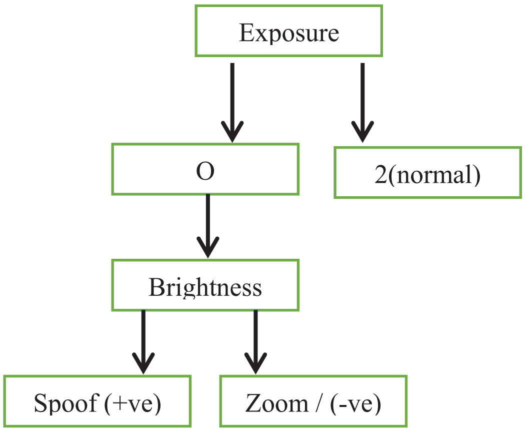


Fig. 1. Flow for Categorization of images based on metadata

Steps For Complete Working Of Program:

```
1. Generate brisque score
2. If score<threshold:
       then original
   else:
      check metadata
3. If metadata>exposure is non zero:
      then original
   else:
      check brightness value
4. If brightness is negative:
      then original
   else:
      fake/altered/corrupted
```

We have used the BRISQUE implementation provided by krshrimali [2] which is an implementation based on [1]. They are basically calculating a score for input image using NSS and SVM together. Figure 2 shows the complete flow of how an image is classified.

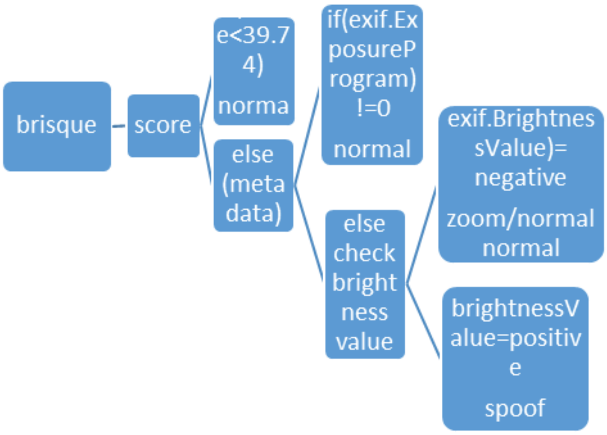


Fig. 2. Complete Flow Image Spoof Detection

IV. RESULTS AND DISCUSSIONS

TABLE II. BRISQUE SCORE FOR IMAGES

Image	Score	Image type
test\157009_5587.jpg	23.65	Normal
test\AXHY3548.JPG	43.61	Normal
test\group1.jpg	25.52	Normal
test\group2.jpg	42.26	zoom/normal
test\group4.jpg	20.15	Normal
test\IMG_20190306_162938.jpg	30.92	Normal
test\IMG_20190306_162952.jpg	58.05	zoom/normal
test\IMG_20190306_163008.jpg	54.01	zoom/normal
test\IMG_20190306_163025.jpg	49.59	zoom/normal
test\IMG_20190306_163049.jpg	50.24	zoom/normal
test\IMG_20190306_163058.jpg	48.41	zoom/normal
test\IMG_20190306_163112.jpg	66.71	zoom/normal
test\IMG_20190306_163121.jpg	60.18	zoom/normal
test\IMG_20190320_114641.jpg	23.55	Normal
test\IMG_20190320_114656.jpg	14.56	Normal
test\IMG_20190403_114311.jpg	63.63	zoom/normal
test\IMG_20190403_114320.jpg	33.55	Normal
test\IMG_20190403_114334.jpg	60.35	zoom/normal
test\IMG_20190403_114343.jpg	36.19	Normal
test\IMG_20190403_114354.jpg	62.88	zoom/normal
test\IMG_5961.JPG	33.02	Normal
test\IMG_5963.JPG	32.22	Normal
test\IMG_8878.JPG	33.41	Normal
test\IMG_8879.JPG	31.68	Normal
test\IMG_8880.JPG	31.89	Normal
test\IMG_8883.JPG	44.22	zoom/normal
test\IMG_8884.JPG	43.95	zoom/normal
test\prashant.jpg	42.96	Edited
test\test.jpg	39.74	Crop/cut
test\test1.jpg	40.48	spoof
test\test2.jpg	57.45	spoof

Table II contains the predicted image scores using BRISQUE for some of our input images. Labeling (Image type) of the image is done by us to compare the end results. The highlighted values represent the images where "Metadata check" needs to be applied to classify the image as a spoof or normal.

TABLE III. FINDINGS ON UPLOAD FOLDER IMAGES

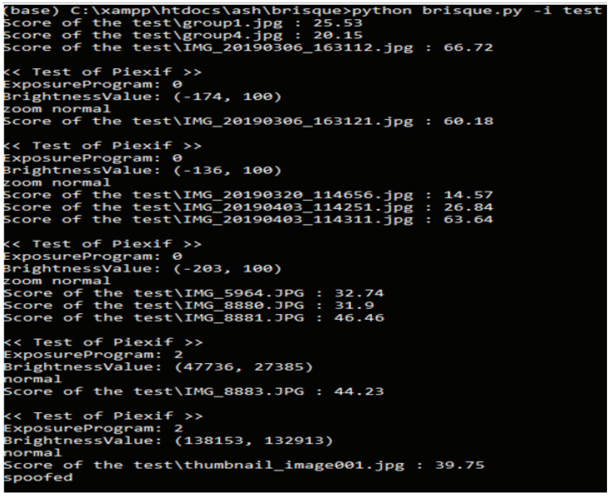
Upload folder images		
Image type	**Image**	**Exif.Exposureprogram**
Normal	Admin20191017_124423/2787	2
Normal	Admin20191017_124423/8725	2
Normal	ADMIN_20191017_152502/5185	2
Normal	ADMIN_20191017_152502/7850	2
Normal	ADMIN_20191017_153943/1911	2
Normal	ADMIN_20191017_153943/6290	2
Normal	ADMIN_20191018_172455/1635	2
Normal	ADMIN_20191018_172607/7777	2

Table III contains the images that all are classified as normal as per the Exposure Program parameter of metadata. Since, Exposure Program is "non-zero", we don't have to check other parameter.

TABLE IV. FINDINGS ON TEST FOLDER IMAGES

Test folder images			
Image type	**Image**	**Exif.Exposureprogram**	**Exif.Brightness value**
Normal	5963	2	
Normal	114656	2	
normal	IMG_8884	2	
Zoom/normal	163025	0	-233/100
Zoom/normal	163121	0	-136/100
Spoof	Test1	0	238/100
Spoof	Test2	0	139/100
Cut	Test	No info	No info
edited	raoof	No info	No info

Table IV contains the data after applying Brightness parameter of metadata. Comparing tables II and IV, we can see how metadata values helped in categorizing the images. For clarification, data highlighted in "aqua" color was labelled as spoof in table II and also categorized as a spoof by applying Meta-Brisque. Cut/ cropped/ edited images don't have any metadata information regarding brightness and Exposure program parameters. So, we can also classify them.



```
(base) C:\xampp\htdocs\ash\brisque>python brisque.py -i test
Score of the test\group1.jpg : 25.53
Score of the test\group4.jpg : 20.15
Score of the test\IMG_20190306_163112.jpg : 66.72

<< Test of Piexif >>
ExposureProgram: 0
BrightnessValue: (-174, 100)
zoom normal
Score of the test\IMG_20190306_163121.jpg : 60.18

<< Test of Piexif >>
ExposureProgram: 0
BrightnessValue: (-136, 100)
zoom normal
Score of the test\IMG_20190320_114656.jpg : 14.57
Score of the test\IMG_20190403_114251.jpg : 26.84
Score of the test\IMG_20190403_114311.jpg : 63.64

<< Test of Piexif >>
ExposureProgram: 0
BrightnessValue: (-203, 100)
zoom normal
Score of the test\IMG_5964.JPG : 32.74
Score of the test\IMG_8880.JPG : 31.9
Score of the test\IMG_8881.JPG : 46.46

<< Test of Piexif >>
ExposureProgram: 2
BrightnessValue: (47736, 27385)
normal
Score of the test\IMG_8883.JPG : 44.23

<< Test of Piexif >>
ExposureProgram: 2
BrightnessValue: (138153, 132913)
normal
Score of the test\thumbnail_image001.jpg : 39.75
spoofed
```

Fig. 3. : Program output of the Meta-BRISQUE code

Figure 3 is the program execution output of the entire process and how the results were obtained.

V. CONCLUSION

In this work, we tried to provide an extended image spoofing solution with BRISQUE for Facial Detection & Recognition systems along with a list of publicly available anti-spoofing Image Databases. Currently, this method was tested for printed attacks which showed outcomes as per our need. Comparison with other algorithms is shown in Table V and the results shows it worked efficiently in terms of execution time as well as accuracy.

TABLE V. COMPARISON OF OTHER SPOOFING ALGORITHMS

Algorithm	Execution time (seconds)	Accuracy
PSNR	0.05	0.86
DIIVINE	120	0.92
BLIINDS	60	0.91
CNN-vgg16 model	40	0.96
BRISQUE	1	0.93
Meta-BRISQUE	4	0.95

REFERENCES

[1] Mittal, A. K. Moorthy & A. C. Bovik (2012). No-reference image quality assessment in the spatial domain. IEEE Transactions on image processing, 21(12), 4695-4708.

[2] No-Reference-Image-Quality-Assessment-using-BRISQUE Model", github.com, https://github.com/krshrimali/No-Reference-Image-Quality-Assessment-using-BRISQUE-Model. [active as of 27/01/2020]

[3] J. Määttä, A. Hadid & M. Pietikäinen (2012). Face spoofing detection from single images using texture and local shape analysis. *IET biometrics*, *1*(1), 3-10.

[4] V. Costa, A. Sousa & A. Reis (2018, November). Image-Based Object Spoofing Detection. In *International Workshop on Combinatorial Image Analysis* (pp. 189-201). Springer, Cham.

[5] Y. Atoum, Y. Liu, A. Jourabloo & X. Liu (2017, October). Face anti-spoofing using patch and depth-based CNNs. In *2017 IEEE International Joint Conference on Biometrics (IJCB)* (pp. 319-328). IEEE.

[6] D. Wen, H. Han & A. K. Jain (2015). Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, *10*(4), 746-761.

[7] M. Diviya & S. Mishra (2016, March). A novel approach for detecting facial image spoofing using local ternary pattern. In *2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM)* (pp. 61-66). IEEE.

[8] Z. Xu, S. Li & W. Deng (2015, November). Learning temporal features using LSTM-CNN architecture for face anti-spoofing. In *2015 3rd IAPR Asian Conference on Pattern Recognition (ACPR)* (pp. 141-145). IEEE.

[9] Z. Sun, L. Sun & Q. Li (2018, April). Investigation in Spatial-Temporal Domain for Face Spoof Detection. In *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 1538-1542). IEEE.

[10] M. Asim, Z. Ming & M. Y. Javed (2017, June). CNN based spatio-temporal feature extraction for face anti-spoofing. In *2017 2nd International Conference on Image, Vision and Computing (ICIVC)* (pp. 234-238). IEEE.

[11] O. Lucena, A. Junior, V. Moia, R. Souza, E. Valle & R. Lotufo (2017, July). Transfer learning using convolutional neural networks for face anti-spoofing. In *International Conference Image Analysis and Recognition* (pp. 27-34). Springer, Cham.

[12] L. Feng, L. M. Po, Y. Li, X. Xu, F. Yuan, T. C. H. Cheung & K. W. Cheung (2016). Integration of image quality and motion cues for face anti-spoofing: A neural network approach. *Journal of Visual Communication and Image Representation*, *38*, 451-460.

[13] Y. Wang, F. Nian, T. Li, Z. Meng & K. Wang (2017). Robust face anti-spoofing with depth information. *Journal of Visual Communication and Image Representation*, *49*, 332-337.

[14] X. Tu & Y. Fang (2017, November). Ultra-deep neural network for face anti-spoofing. In *International Conference on Neural Information Processing* (pp. 686-695). Springer, Cham.

[15] J. Gan, S. Li, Y. Zhai & C. Liu (2017, March). 3D convolutional neural network based on face anti-spoofing. In *2017 2nd international conference on multimedia and image processing (ICMIP)* (pp. 1-5). IEEE.

[16] Maksymenko S. "Anti-Spoofing Techniques For Face Recognition Solutions", Towards Data Science,

[17] https://towardsdatascience.com/anti-spoofing-techniques-for-face-recognition-solutions-4257c5b1dfc9, [active as of 27/01/2020