DOI: 10.2352/ISSN.2470-1173.2016.2.VIPC-242

Fingerprint Liveness Detection Using Ensemble of Local Image Quality Assessments

Wonjun Kim, Sungjoo Suh, Youngsung Kim, and Changkyu Choi
Software Solution Lab., Samsung Advanced Institute of Technology (SAIT), Suwon-si, Gyeonggi-do 443-803, South Korea

Abstract

Detecting spoofing compared to a live trait is a critical problem in the biometric authentication. In this paper, we present a novel method to detect fake fingerprint attacks based on the ensemble of image quality assessments (IQAs). The key idea of the proposed method is to combine quality scores obtained from multiple local regions, which are input into the linear SVM classifier to determine whether the given fingerprint is fake or not. One important advantage of the proposed method is that, in contrast to previous approaches, it accurately identifies fake fingerprints even with small partial distortions. Moreover, the proposed method does not require any additional device. Experimental results on the mobile device show that the proposed method is effective for fingerprint liveness detection in real-world scenarios.

Introduction

In recent years, the biometric-based authentication on mobile devices has gained considerable attention because of their inherent traits. Therefore, various biometric systems have been actively researched and are now deployed in high-level security systems. Among the different biometics analyzed, the face and fingerprint-based user verifications have been most actively exploited for the mobile applications such as unlock screen and payment. However, the face-based framework is easily attacked by photographs and videos simply acquired in the web site (also vulnerable to the large range of intra-class variation due to diverse poses, illuminations, and expressions) [1] and thus hardly employed for the user verification on the smartphone. Even though the fingerprint-based verification is successfully commercialized based on the reliable performance, it still suffers from malicious spoofing attacks by a variety of materials, e.g., play-doh, silicon, gelatin, wood glue, etc. To resolve this problem, the software-based methods start to be popularly studied. Specifically, Abhyankar and Schuckers [2] focused on the ridge characteristics with the first order texture information, e.g., entropy, variance, skewness, etc. They encode these components by utilizing the fuzzy c-means clustering to discriminate live fingerprints from fake ones. In [3], authors combined the perspiration (i.e., pore characteristics) and morphological features for fingerprint liveness detection. Jia *et al.* [4] proposed to adopt the local binary patterns (LBP) for describing the difference between live and fake fingerprints. Even though such texture-based approaches are conceptually simple and effective when a single image is used, they are vulnerable to high resolution-based spoofing attacks. Most notably, Galbally *et al.* [5] applied the image quality assessment (IQA) for fake biometric detection in a global manner. Specifically, they attempted to combine full reference-based IQA schemes with no reference-based ones. However, this method is vulnerable to the local distortion due to the nonuniformity of materials as well as variable pressures since they only consider the quality of the whole image. Some examples of fake fingerprints are shown in Fig. 1.

Figure 1. *A simple examples of fake fingerprints (images from the LivDet09 database, which is available at http://prag.diee.unica.it/LivDet09. Note that some parts of given images are distorted due to different pressures or impuroties, which lead to the quality degradation.*

In this paper, we present a novel method for fingerprint liveness detection based on the ensemble of locally-computed quality scores. One important advantage of the proposed method is to be robust to local distortions driven by the surface unhomogeneity of fake materials as shown in Fig. 2. More specifically, we divide the given fingerprint image into multiple overlapped blocks and compute the scores of selected IQAs on each blcok. Then, such scores are concatenated into a single feature vector, which is fed into the linear SVM classifier.

Proposed Method

In this section, we explain the proposed method for fingerprint liveness detection in detail. In the state-of-the-art, the rationale behind the use of IQA features for liveness detection is supported by two main factors [5]:

- People highly tend to discriminate the live samples from fake ones based on the "different appearance". Since the IQA models intend to estimate the perceived appearance of given images in an objective and reliable way, they are very suitable for detecting spoofing attacks especially by the fake fingerprint.
- IQAs have been successfully employed in the forensic field such as image manipulation detection [6, 7] and steganalysis [8]. Since making fake fingerprints can be regarded as the procedure of image manipulation, we can expect that IQA-based spoofing detection provides the reliable performance even under attacks based on diverse materials.

Moreover, combining various IQA models leads to exploit complementary image quality properties (e.g., SSQE [12] reveals the texture characteristics while BRISQUE [10] focuses on the loss

DOI: 10.2352/ISSN.2470-1173.2016.2.VIPC-242

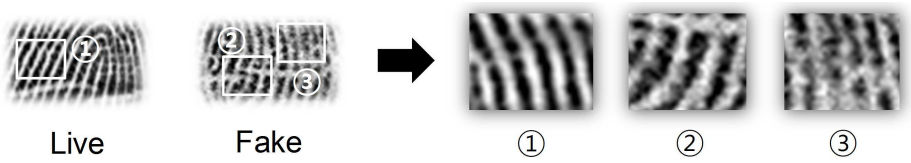

Figure 2. *A simple examples of live and fake fingerprint images captured by the capacitive sensor. Note that the live fingerprint ( ) has different quality compared to the fake one (and).*

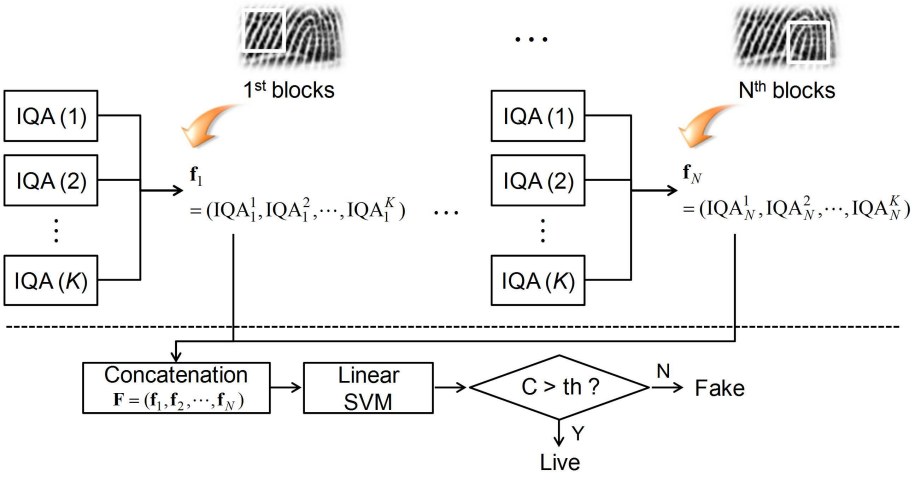

Figure 3. *Overall procedure of the proposed method. Note that we use three IQAs (i.e., $K = 3$ (**BRISQUE**, **NIQE**, **SSQE**)) for each sub-block in our implementation. Therefore, the dimension of the feature vector is $K \times N$. C denotes the confidence value for the corresponding image.*

of naturalness) and thus detect the quality differences between live and fake fingerprints expected to be found in many attack attempts. All the things we observed guarantee that IQA-based spoofing detection has the plentiful possibilities to achieve success in biometric protection tasks.

Overview of the Proposed Method

The motivation of our new approach is to find more effective way for fingerprint liveness detection under the assumption that a fake fingerprint image may have locally different quality compared to a live one due to the acquisition artifacts such as spots and blurring. It follows that the measure of local quality in a given image can provide a good approximation to capture the difference between live and fake fingerprints. Moreover, the image quality assessment (IQA) has been successfully adopted to detect image manipulation, which can be regarded as a type of spoofing attacks [5, 7]. From this point of view, we exploit the ensemble of local quality scores as our features to learn about the different appearance of live and fake fingerprints.

To do this, we allow for the no-reference IQA models, which do not require the reference image and thus suitable for mobile applications. Most of no-reference IQA models estimate the quality of the given image based on some pre-trained statistical models (e.g., natural scene statistic [9]). We select three representative no-reference methods as follows:

- **BRISQUE** [10] : this method does not compute the distortion-specific features such as ringing, blurring or blocking. Instead, it employs the scene statistics estimated by the generalized Gaussian distribution (GGD) to quantify possible losses of naturalness in the image due to the presence of distortions, thereby leading to a holistic measure of quality.
- **NIQE** [11] : unlike BRISQUE requiring the knowledge about estimated distortions in training examples and corresponding human opinion scores, this method only makes use of measurable deviations from statistical regularities observed in natural images without training on human-rated distorted images (i.e., completely blind). It adopts the patch-based GGD scheme to evalute the image quality.
- **SSQE** [12] : this model utilizes the entropy obtained from both spatial and spectral domains for estimating the image quality. For the spectral entropy, they compute the block-based DCT coefficients, and subsequently conduct the feature pooling for the prediction of the quality scores.

It is worth noting that combining those IQAs is desirable to completely represent traits of live and fake fingerprints obtained from both spatial and spectral domains with the multiscale analysis. Moreover, the opinion-aware quality measure also can be reflected in this scheme. The summary of each IQA employed in our implementation is shown in Table. 1. In the following subsection, we will explain the proposed ensemble scheme of local quality scores in detail.

Ensemble of Local Quality Scores

The proposed local quality-based liveness detection is summarized as follows: first of all, we divide the given fingerprint im-

©2016 Society for Imaging Science and Technology
DOI: 10.2352/ISSN.2470-1173.2016.2.VIPC-242

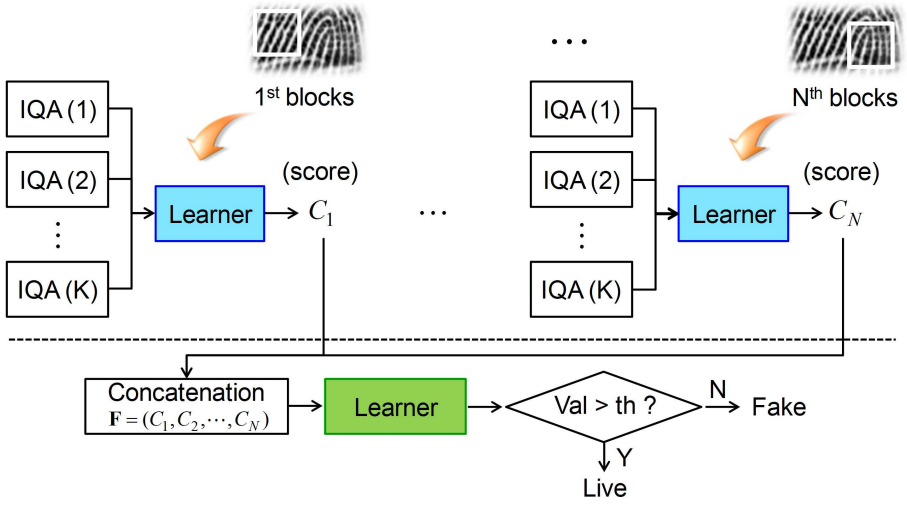

Figure 4. *Overall procedure of the proposed method (late-fusion scheme). For this, we train sub-learner for each sub-block in our implementation. Therefore, the dimension of the feature vector is N. C denotes the confidence value for the corresponding image. Note that it requires more training phases compared to the early fusion shown in Fig. 3 even though this scheme tends to yield better performance.*

Table 1. List of three image quality assessment (IQA) models in the present work for fingerprint liveness detection

	Type	Acronym	Name	Description
1	NR	BRISQUE	Blind/Referenceless Image Spatial Quality Evaluator	Modeling distributions of normalized pixel intensities with the generalized Gaussian model (GGD) with its neighbor relationships
2	NR	NIQE	Natural Image Quality Evaluator	Collecting quality-aware features and fitting them into a multivariate Gaussian (MVG) model
3	NR	SSEQ	Spatial Spectral Entropy based Quality	Predicting scores by pooling entropy features computed from the spatial and spectral domain (particularly based on the DCT coefficients)

NR : no-reference image quality assessment models

age into N overlapped sub-blocks with the size of $W \times H$ pixels (see Fig. 3). Then, we compute the scores of three no-reference IQA models, i.e., **BRISQUE** [10], **NIQE** [11], and **SSEQ** [12], on each sub-block. Since the human visual system (HVS) does not require a reference sample to determine the quality of a given image, we just follow this assumption for our IQA-based spoofing detection scheme. More specifically, **BRISQUE** simply adopts the normalized luminance information without any feature transformation (e.g., DCT, wavelets, etc.) to measure the "naturalness" in the spatial domain. The relationship between pixel intensities are modeled by utilizing the generalized Gaussian model (GGD) (i.e., it requires the training phase) and the quality score is finally computed based on the support vecotr machine (SVM) regressor [13]. **NIQE** defines the natural scene statistics (NSS) based on the intensity-based statistical information (e.g., mean and variance) obtained from local patches of a given image. These features are fitted into the multivariate Gaussian (MVG) model and yield the quality score by using parameters of MVG as follows:

$$D = \sqrt{((v_1 - v_2)^T \left(\frac{\sigma_1 + \sigma_2}{2}\right)^{-1} (v_1 - v_2)}, \quad (1)$$

where v_1, v_2 and σ_1, σ_2 are the mean vectors and covariance matrices of the natural MVG model and the distorted one. It is worth noting that **NIQE** does not require any training phase and thus called "double-blind". Finally, **SSEQ** allows the spatial-spectral entropy for assessing the quality of a distorted image across multiple distortion categories. It divides the given image into non-overlapped $M \times M$ blocks (e.g., $M = 8$) and compute the spatial entropy and spectral one utilizing DCT coefficients as follows:

$$E_s = -\sum_x p(x) \log_2 p(x), \quad (2)$$

$$E_f = -\sum_i \sum_j p(i,j) \log_2 p(i,j), \quad (3)$$

where $p(i,j) = \frac{C(i,j)^2}{\sum_i \sum_j C(i,j)^2}$ and C denotes the matrix of DCT coefficients. x indicates the pixel value with the empirical probability density $p(x)$, which is defined based on the intensity distribution in the local patch. Feature pooling is conducted by using values of spatial and spectral entropies to predict the quality scores. Note that other no-reference IQA models also can be involved into our ensemble scheme without any additional task.

DOI: 10.2352/ISSN.2470-1173.2016.2.VIPC-242

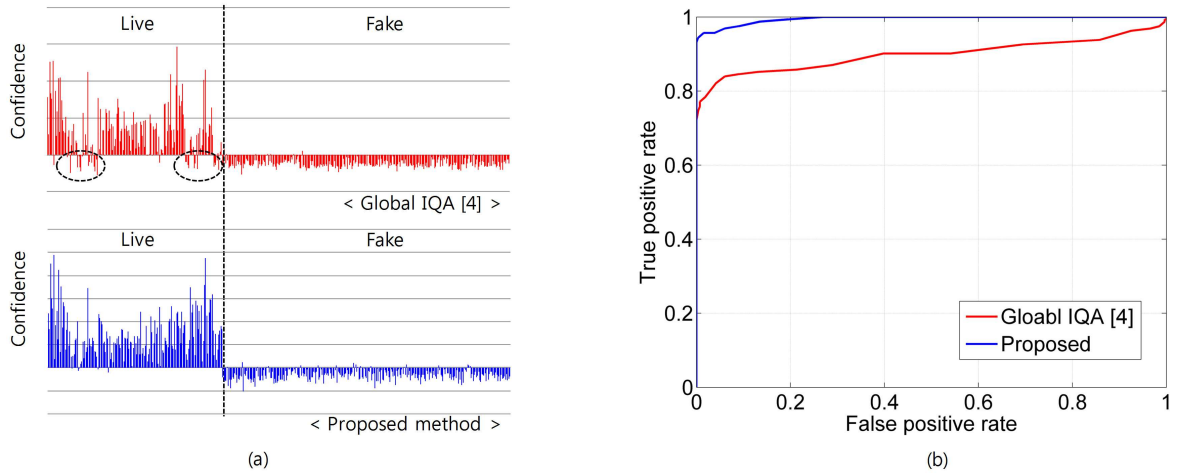

Figure 5. *Performance evaluation. (a) Distributions of confidence values computed from the linear SVM classifier. Note that some significant falsely detected scores occur in the previous method [5] (see the circled regions). (b) ROC curves for the performance comparison (best viewed in colors). We can see that the proposed method has an ability to provide the reliable fake detection performance with the high accuracy at the low-level of the false positive rate.*

The corresponding results (i.e., scores from **BRISQUE**, **NIQE**, and **SSEQ**) are concatenated on each block and formulated as follows:

$$\mathbf{F} = (\mathbf{f}_1, \mathbf{f}_2, \cdots, \mathbf{f}_N), \quad \text{where} \quad \mathbf{f}_i = (S_i^B, S_i^N, S_i^S). \tag{4}$$

Here S^B,S^N, and S^S denote the scores of **BRISQUE**, **NIQE**, and **SSEQ** in the ith sub-block, respectively. Therefore, the feature dimension is set to $N \times 3$ in our method. The feature vector $\mathbf{F}$ is fed into the linear SVM classifier to learn about the difference between live and fake fingerprints. The overall procedure of the proposed method is shown in Fig. 3. Furthermore, the proposed approach can be efficiently incorporated into the late-fusion scheme. That is, a single score of each block, which is driven by **BRISQUE**, **NIQE**, and **SSEQ**, respectively, is separately trained. The corresponding confidence values can be concatenated and defined as our feature, which is fed into the linear SVM classifier once again. Note that the late-fusion scheme is apt to yielding the slightly better performance in visual recognition tasks [14], however, it requires more training phases as mentioned, which is time-consuming. The overall procedure of the late-fusion based scheme is shown in Fig. 4. It should be emphasized that our focus is not to design the IQA models but to efficiently combine their scores.

Experimental Results

In this section, we demonstrate the performance of the proposed method based on our fingerprint liveness (SFL) dataset. The SFL dataset is constructed by utilizing the capacitive-based fingerprint sensor under real-world situations. For generating the fake fingerprint, we attempt to combine the wood glue with the graphite, and thinly cut the surface of the fingerprint. Since play-doh and silicon hardly transfer the electric signals, those are not suitable for our experiments. In the SFL dataset, 324 fingerprints (live: 162 images / fake: 162 images) were collected for training while the test dataset comprised 429 fingerprints (live: 162 images / fake: 267 images). It should be noted that these are mutually exclusive. Based on the extensive experiments, we divide the fingerprint image into 10 sub-blocks with the small amount of the overlap area (i.e., $N = 10$ in (4) with the 8-pixel overlap).

Table 2. Performance comparison of fingerprint liveness detection on the SFL dataset

Method	Live	Fake	Accuracy
Global IQA [5]	130/162	259/267	90.68%
Proposed	157/162	247/267	**94.17%**

Table 3. Detection accuracy at the FAR = 1%

Method	Global IQA [5]	Proposed
FAR=1%	78.40%	**95.68%**

For the quantitative evaluation, we compare the proposed method with the most competitive approach in the literature [5] based on the early fusion scheme as shown in Fig. 3. The corresponding results are shown in Fig. 5 and Table 2, respectively. Specifically, we first show the confidence value of the linear SVM classifier for both methods in Fig. 5(a). As can be seen, the previous method often fails to detect the live fingerprint while the proposed scheme provides more reliable results for fingerprint liveness detection. The correponding ROC curves are also shown in Fig. 5(b). The detection accuracy is shown in Table 2 in detail. We can see that the proposed method has an ability to accurately discriminate fake fingerprints from live ones even with the presence of small distortion parts. In addition, we also check the performance at the level of 0.1 false positive rate (i.e., FAR = 1%) and the comparison results are shown in Table 3. Since the protected system requires high-level security, anti-spoofing methods need to strongly reduce falsely accepted cases. Therefore, it is thought that our approach can be efficiently applied to various mobile applications. Some examples of misclassification on our SFL dataset are shown in Fig. 6. Note that these two cases are hardly discriminated from each other based on the image quality.

DOI: 10.2352/ISSN.2470-1173.2016.2.VIPC-242

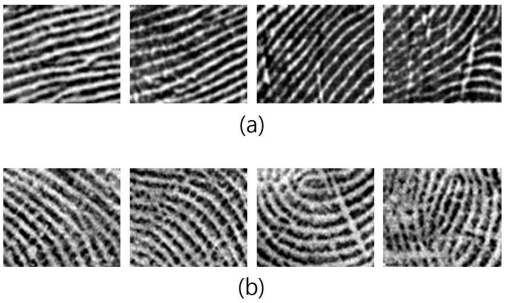

Figure 6. *Some examples of misclassification on the SFL dataset. (a) Live but falsely detected as fake. (b) fake but falsely detected as live. Note that thses two cases are hardly discriminated from each other.*

Discussion

In order to improve the detection performance, full-reference IQA models, which require both live and fake fingerprint images simultaneously, can be incorporated into the proposed framework. Since users generally enroll their "live" fingerprints for the smartphone, we can reliably construct the spoofing-free model based on such enrolled information. When fingerprint images are input to the device, the proposed method may attempt to detect whether a given image is live or fake based on the stored spoofing-free model. In this point of view, we can employ a variety of full-reference IQA models, e.g., from simple difference-based metrics (MSE [15], PSNR [16], maximum difference [17], total edge difference [18], etc.) to the structured metrics (**SSIM** [19], **VIF** [20], and **RRED** [21]), with our main features (i.e., scores from **BRISQUE**, **NIQE**, and **SSEQ**). However, full-reference IQA models require the additional memory space and thus we need to consider the combining strategy for the memory-limited environment of the mobile device in a very efficient way. To alleviate this problem, we can allow for the alternative combination scheme, i.e., full-reference IQA models computed in a global manner while our features are obtained from local patches.

Conclusion

A novel method for fingerprint liveness detection has been proposed in this paper. The key idea behind the proposed approach is that the difference between traits of live and fake fingerprints is well revealed in a quality-aware manner. To this end, we first divide the given image into multiple sub-blocks and compute the quality scores by exploiting three representative image quality assessment (IQA) models. By concatenating those quality scores, we define our feature vector, which is fed into the linear SVM classifier. Experimental results show that the proposed method successfully discriminates fake fingerprints from live ones. Our future work is to incorporate full-reference IQA models into the proposed framework without the significant increase of the memory usage.

References

[1] W. Kim, S. Suh, and J-J. Han, "Face liveness detection from a single image via diffusion speed model," *IEEE Transactions on Image Processing*, vol. 24, no. 8, pp. 2456-2465, Aug. 2015.

[2] A. Abhyankar and S. Schuckers, "Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques," in *Proc. IEEE International Conference on Image Processing (ICIP)*, pp. 321-324, Oct. 2006.

[3] E. Marasco and C. Sansone, 'Combining perspiration- and morphology-based static features for fingerprint liveness detection," *Pattern Recognition Letters*, vo. 33, no. 9, pp. 1148-1156, Sept. 2012.

[4] X. Jia et al., "Multi-scale block local tenary patterns for fingerprints vitality detection," in *Proc. International Conference on Biometrics (ICB)*, pp. 1-6, June 2013.

[5] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition," *IEEE Transactions on Image Processing*, vol. 23, no. 2, pp. 710-724, Feb. 2014.

[6] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," *Journal of Electronic Imaging*, vol. 15, no. 4, pp. 041102-1-041102-17, 2006.

[7] M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulcation using statistical intrinsic fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 492-496, Mar. 2010.

[8] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," *IEEE Transactions on Image Processing*, vol. 12, no. 2, pp. 221-229, Feb. 2003.

[9] A. K. Moorthy and A. C. Bovik, "A two-step framework for constructing blind image quality indices," *IEEE Signal Processing Letters*, vol. 17, no. 5, pp. 513-516, May 2010.

[10] A. Mittal, A. K. Moorthy, and A. C. Bovik, "No-reference image quality assessment in the spatial domain," *IEEE Transactions on Image Processing*, vol. 21, no. 12, pp. 4695-4708, Dec. 2012.

[11] A. Mittal, R. Soundararajan, and A. C. Bovik, "Making a completely blind image quality analyzer," *IEEE Signal Processing Letters*, vol. 20, no. 3, pp. 209-212, Mar. 2013.

[12] L. Liu, B. Liu, H. Huang, and A. C. Bovik, "No-reference image quality assessment based on spatial and spectral entropies," *Signal Processing: Image Communication*, vol. 29, no. 8, pp. 856-863, Aug. 2014.

[13] B. Scholkopf, A. J. Smola, R. C. Williamson, and P. L. Bartlett, "New support vector algorithms," *Neural Computing*, vol. 12, no. 5, pp. 1207-1245, 2000.

[14] C. G.M. Snoek, M. Worring, and A. W. M. Smeulders, "Early versus late fusion in semantic video analysis," in *Proc. ACM International Conference on Multimedia*, pp. 399-402, 2005.

[15] I. Avcibas, B. Sankur, and K. Sayood, "Statistical evaluation of image quality measures," *Journal of Electronic Imaging*, vol. 11, no. 2, pp. 206-223, 2002.

[16] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," *Electronics Letters*, vol. 44, no. 13, pp. 800-801, 2008.

[17] A. M. Eskicioglu and P. S. Fisher, "Image quality measures and their performance," *IEEE Transactions on Communications*, vol. 43, no. 12, pp. 2959-2965, Dec. 1995.

[18] M. G. Martini, C. T. Hewage, and B. Villarini, "Image quality assessment based on edge preservation," *Signal Processing: Image Communication*, vol. 27, no. 8, pp. 875-882, 2012.

[19] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600-611, Apr. 2004.

[20] H. R. Sheikh and A. C. Bovik, "Image information and visual quality," *IEEE Transactions on Image Processing*, vol. 15, no. 2, pp. 430-

DOI: 10.2352/ISSN.2470-1173.2016.2.VIPC-242

444, Feb. 2006.

[21] R. Soundararajan and A. C. Bovikl, "RRED indices: Reduced reference entropic differencing for image quality assessment," *IEEE Transactions on Image Processing*, vol. 21, no. 2, pp. 517-526, Feb. 2012.