Topological Data Analysis for Image Tampering Detection

Aras Asaad(✉) and Sabah Jassim(✉)

Applied Computing Department,
The University of Buckingham, Buckingham, UK
{aras.asaad, sabah.jassim}@buckingham.ac.uk

Abstract. This paper introduces a topological approach to detection of image tampering for forensics purposes. This is based on the emerging Topological Data Analysis (TDA) concept of persistent homological invariants associated with certain image features. Image features of interest are pixels that have a uniform Local Binary pattern (LBP) code representing texture feature descriptors. We construct the sequence of simplicial complexes for increasing sequence of distance thresholds whose vertices are the selected set of pixels, and calculate the corresponding non-increasing sequence of homology invariants (number of connected components). The persistent homology of this construction describes the speed with which the sequence terminates, and our tamper detection scheme exploit its sensitivity to image tampering/degradation. We test the performance of this approach on a sufficiently large image dataset from a benchmark dataset of passport photos, and show that the persistent homology sequence defines a discriminating criterion for the morphing attacks (i.e. distinguishing morphed images from genuine ones).

Keywords: Topological Data Analysis · Persistent homology · Image tampering · Image morphing

1 Introduction

Digital image morphing is an image tampering attack that form a serious threat to the security of ID token based verification when applied to face photos. Morphing is the process of transforming one digital image into another digital image. Several powerful hardware and software tools are available for creating and manipulating images easily without leaving any noticeable noises on the digital image and thereby undermining the authenticity and integrity of digital images. When face images are used as evidence of person proofs then one can no longer take the authenticity of the face images for granted. Morphing can also be used to attack face biometric systems with adverse influence on recognition accuracy as a result of allowing non-authorized persons to access or pass the recognition system. This presents a serious challenge to the digital forensics community: how to distinguish a genuine source face image from a morphed image and prevent subsequent security breaches.

Ferrara et al. in [1] introduced morphing attack as a major security concern which can bypass all integrity checks (optical and electronic). The study illustrated that,

C. Kraetzer et al. (Eds.): IWDW 2017, LNCS 10431, pp. 136–146, 2017.
DOI: 10.1007/978-3-319-64185-0_11

Automatic Border Control (ABC) systems as well as human experts can be deceived by presenting a passport with a morphed face photo on it whereby they concluded that two persons can share one passport. Morphed images in [1] have been created by the freely available GNU Image manipulation software v2.8 (GIMP) [2] and the GIMP animation Package v2.6 (GAP) [3]. To evaluate the recognition systems, they tested the quality of morph images by two commercial tools: Neurotechnology VeryLook SDK 5.4 and Luxand Face SDK 4.0.

The morphing described in [1, 4] are time consuming because it requires a manual retouch for more realistic appearance. To overcome this issue, Makrushin et al. in [5] proposed an automatic splicing-based morphing algorithm to generate thousands of visually faultless facial morphs. In general, the quality of morphed images is 2-fold; (i) morphed images need to be visually faultless to human eyes (i.e. no visible artefacts) and (ii) morphs should be successfully verified against both source images by automatic face recognition systems. The splicing morph technique is a result of warping and alpha-blending of segmented facial regions and seamlessly stitching it back into one of the input (source) images. This approach is different from the complete morphing technique which takes the complete facial image to warp and blend including hair and background. Splicing morph result in a more natural looking image than the complete morph technique which cause the appearance of spurious shadows. Nonetheless, the geometry of splicing morphs is taken completely from one source image and it has minor ghosting artefacts which caused by inaccurate localization of facial landmarks. Also, if the skin color is different for both source images, a splice morph does not look realistic. These properties make splicing technique to pass the first morph quality measure, provided that both source images have similar skin color, but miserable regarding the second quality measure because splicing adopts geometry from one source image only and it may not look very similar to the other image. A combined morph technique was also proposed by [5] to overcome the limitations in the two previous algorithms. It warps the images into an average position first, then it cuts the facial regions, blending and finally stitching them back on to the warped image. Poison image editing will be applied as a final stage to obtain seamless transmission between the facial region and the rest of the image. Combined morph images have an average geometry and texture from both source images but has no major ghosting artefacts and skin color has no influence.

Different morphing techniques are expected to produce different changes on image features, and potential digital forensic schemes to detect morphing must identify the appropriate sensitive features and the nature of resulting changes in order to select appropriate classifiers. Makrushin et al. in [5] proposed an automatic morph detector based on Benford features computed from quantized Discrete Cosine Transformation (DCT) coefficients of JPEG-Compressed images. Frank Benford's law, roughly, states that the frequency distribution of leading digits of a set of (natural) numbers is logarithmic. The morphing detector adopted in [5] is based on the hypothesis that unlike naturally generated data, manipulated data do not obey the Benford's law. Although high accuracy in detection of morphed random face images obtained using Benford's law, however, they note that using legitimate image processing techniques, one can create face images with similar Benford feature distribution [5, 6].

In this work, we shall investigate the use of Topological Data Analysis based schemes that systematically construct the topological shapes associated with a given set of specific texture pixels distributed spatially in an image. We shall test the possibility of using the well-known persistent homology invariant relating to the number of connected components in the incrementally constructed sequences of shapes as a morphing predictor. We shall focus on using face images produced by three different types of morphing schemes (splicing, combined and complete morphing methods). Our proposed approach is based on the topology of texture descriptors, known as local binary patterns, of face images.

The rest of the paper organized as follows. Section 2 encompasses the topological data (image) analysis including recent applications of this emerging scheme. Local binary patterns are introduced in Sect. 3 as an image texture descriptor to build Rips complexes. In Sect. 4, our proposed method to detect image tampering introduced together with experimental results. Finally, Sect. 5 reports the conclusion and future directions.

2 Topological Data/Image Analysis

Topology is a field of mathematics that is concerned with the classification of shapes (objects) according to their closeness and connectivity properties. In recent years, the emergence of machine learning for the analysis of Bigdata has energized interest in utilizing shape and topology of data in complex classification applications. Understanding and classifying shape relies on expressing complex shapes in terms of simple shape building blocks using easy to implement combinatorial construction methods. Topological Data Analysis is concerned with such challenges [7, 8, 14]. Topologists have long developed a finite combinatorial process known as simplicial complex, which can be used to construct the topological shape of datasets of points in any metric space. Roughly speaking, simplicial complex takes a set of points (0-dimensional simplices), edges (1-dimensional simplices), triangles (2-dimensional simplices) and hyper-dimensional triangles and glue them together along their edges and faces to make complex patterns conveying connectivity and closeness properties. The fundamental idea behind using topology for data analysis is that via topology, one can extract shapes, or patterns, from complex high dimensional data sets and then obtaining deep intuitive understanding about them. Topology has three key properties which enables extracting patterns, or shapes, possible form high-dimensional data sets. These properties are; coordinate free, invariant under (small) deformation and compressed representation [8]. These three important properties of topology have been discussed in detail in [7, 8]. Recent application scope of topological data/image analysis includes, but is not limited to, gait recognition [9, 10, 22], brain artery [20], hurricane and galaxies analysis [11], dimensionality reduction schemes evaluation [12], classification of hepatic lesions [21], shape classification using LBP and persistent [13] and many more.

Topological properties of objects/shapes can be characterized by their homology. In general, to distinguish distinct objects from one another, one needs to use homology to measure the number of connected components, loops, and voids of those objects. The focus of this paper is mainly about computing the number of connected components of specific uniform LBP patterns from constructed simplicial complexes of face images. Mathematically, zero homology groups associated with simplicial complexes are basically equals to number of connected components. Persistent refers to constructing more than one simplicial complex from specific LBP patterns using different distance thresholds. The properties (features) of face images that persist (survive) after changing these thresholds, which will result in different simplicial complex structures, will be treated as a true property of that image. In this work, we will focus on computing persistent homology of Rips complexes as a morph detector constructed from a selected group of uniform LBP pattern which is the case of having two ones in the LBP code. In particular, the type of simplicial complex which will be built is known as Vietoris-Rips simplicial complex (or Rips complex). In order to construct and calculate the corresponding non-increasing sequence of homology invariants of Rips complex one needs to select a distance threshold (parameter) T as a first step of the construction.

Then gradually increasing T, higher dimensional simplices will be constructed. For sufficiently small T, only zero dimensional simplices will be obtained and for sufficiently large T, a single high dimensional simplex (object) will be constructed. The features that are surviving after changing the threshold are considered to be true features conveying information about morphing face images. The features that are not persistent by gradually increasing the threshold considered to be noise [7, 19]. This approach is known as persistent homology where at each distance threshold, homology invariants will be computed for the image of interest to make decision about being a morph or a genuine photo image.

3 Local Binary Patterns (LBP)

Local Binary pattern is an image texture descriptor which has been first introduced by Ojala et al. [15], but since then a variety of versions have been investigated and used in pattern recognition with considerable success. Given any image I, the original LBP generates a new image by associating with each pixel an 8-bit binary code determined by comparing its value with that of its 8 neighbors in a 3×3 window surrounding it in a clockwise order as illustrated in Fig. 1. The process works by first subtracting the central pixel value from the 8 neighboring pixels, and starting from the top left corner neighbor each cell is assigned 0 or 1 depending whether the subtraction outcome is negative or not. The LBP codes can be converted back to their decimal values representing the central pixel (x_c, y_c) using Eqs. (1) and (2), below:

$$LBP(x_c, y_c) = \sum_{i=0}^{i=7} \alpha(P_i - P_c)2^i \tag{1}$$

where P_i is the neighbouring grey value pixels, P_c is the centre grey value pixel and the function $\alpha(x)$ is as follow:

$$\alpha(x) = \begin{cases} 1 \ \mathit{if} x \geq 0 \\ 0 \ \mathit{if} x < 0 \end{cases} \tag{2}$$

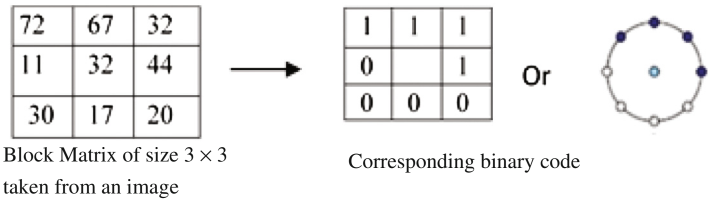

Fig. 1. Local binary operator

Applying above procedure on the block matrix will result in getting the binary string 11110000 (decimal = 15), see Fig. 1.

Local texture information, such as edges, lines, spots and flat regions are associated with certain types of LBP codes named, by Ojala et al. as uniform patterns referring to 8-bit circular bytes that contain either 0 or 2 bitwise transitions from 1 to 0 and from 0 to 1. For example, 11111111 (0-transition) and 00111111 (2-transitions) are uniform codes while 10111010 is non-uniform as it has 6 transitions. A circular 8-bit string are uniform if it contains a single run of 1's of a fixed length k, with k = 0, 1, 2, … 8. It is not difficult to show that the LBP of any monochrome image consists of 58 distinct uniform patterns. Ojala et al. [15], experimentally demonstrated that 90.6% of all LBP patterns in texture images are uniform and postulated that the histogram of the uniform LBP patterns is useful as a discriminating feature in image classification applications. Ahonen et al. [16], Shan et al. [17], and Meng et al. [18] have used the histogram of the uniform LBP bins as discriminating features for face recognition and facial expression recognition. Indeed, currently variations of this LBP-based scheme is adopted widely in a variety of pattern recognition schemes whenever image texture is an important image feature for the relevant application.

In this paper, we investigate the use of topological invariants of Rips simplicial complexes associated with uniform LBP pixels at different distance thresholds for the detection of morphing attacks on passport photos. Image tampering and morphing in particular is expected to result in a variety of changes to the position of the different uniform LBP codes which in return result in changing the corresponding simplicial complexes. The fact that over 90% of the LBP codes of a face image are expected to be uniform, constructing and quantifying the homological invariants of their Rips complexes is a rather daunting task. Instead, investigating the complexes constructed from specific and closely related groups of uniform codes is a more tractable task. Excluding, the two rather trivial uniform LBP codes of 0000000 and 11111111, the remaining 56 uniform codes can be divided into 7 groups of uniform codes where each group consists of codes with the same number of 1's. Each of the 7 groups consists of 8 LBP codes that can all be generated from a single one by rotation. By examining several images we noted some interesting statistical relations between uniform codes across the 7 groups, which may be exploited to determine the sensitivity of their topological invariants to image tampering. Figure 2, below illustrates this idea by showing the

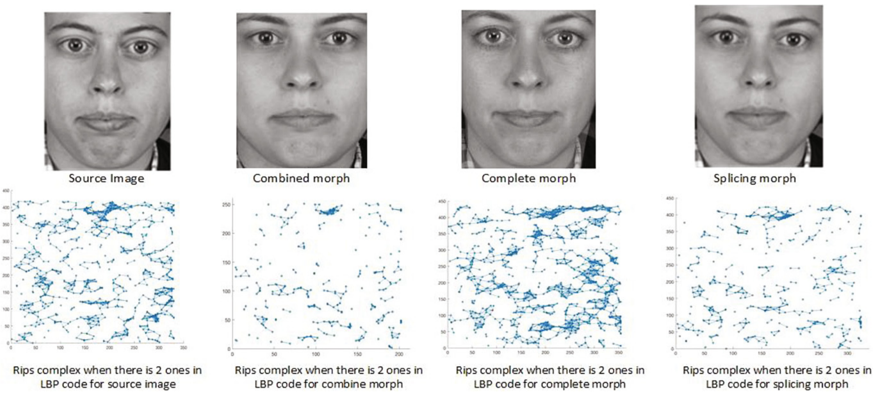

Fig. 2. Sensitivity of topological invariants to morphing

simplicial complexes constructed from the positions of a single uniform LBP code for an original image and its 3 different morphs with another face image.

We initialized our TDA based investigations by focusing first on homological invariants of the sequence of simplicial complexes associated with the group of 2-ones uniform LBP codes depicted in Fig. 3. This group is known to be associated with the geometric structure of an end of a line, and hence it is expected to play a significant role as image discriminating feature. In the rest of the paper, we shall investigate the sensitivity to morphing attacks of the threshold-dependent simplicial complexes constructed from this group of uniform LBP codes.

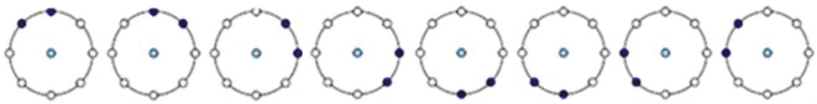

Fig. 3. Uniform LBP group of 2-Ones where dark nodes indicate the position of 1.

4 Proposed Method

In this section, we describe the two main components of our topological proposal to detect image tampering. The first component is the procedure for constructing the threshold-dependent sequence of simplicial complexes associated with any input set of pixel points in an image. The second component describes our simplified analyses of the corresponding sequence of a chosen topological invariants for detecting image tampering. And we present the results of our experiments on relevant database of face images, where we chose each of the uniform 2-ones LBP pixel points, and the number of connected components as the topological invariant.

4.1 Construction of Rips Simplicial Complexes

Given a set of selected image pixel positions $P = \{p_1(x_1, y_1), p_2(x_2, y_2), \ldots, p_n(x_n, y_n)\}$. First compute the Euclidian distance between all pairs of points in the set, and determine the minimum and maximum distance values T_{min} and T_{max}. In the interval $[T_{min}, T_{max}]$ select k equidistant thresholds $\{T_1 = T_{min}, T_2, \ldots, T_k = T_{max}\}$. For simplicity we fix $k = 30$ for the purpose of persistent computation, but this number could be changed if need be. Start by iteratively constructing a simplicial complex by joining each pairs of points in P if the distance t between them satisfy the relation $T_{i-1} < t \leq T_i$ where $i = 2, \ldots, k$. Compute the number cc_i of connected components. If $cc_i = 1$ then stop else increment I and repeat. The output from this procedure is the sequence $(cc_0, cc_1, cc_2, \ldots cc_k)$, where $cc_i = \#(P)$ and $cc_k = 1$ represents the terminating threshold. Note that, different point sets may have different threshold intervals and different length sequences.

This procedure yields a sequence of graphs consisting of the 0-simplicies represented by the set P and the 1-simplices representing the added edges. At each step, this construction only generates 1-skeleton of the full Rips simplicial complex which is sufficient for the current purpose, but the full complex requires the addition of all possible higher dimensional simplices. For example, every 3 points form a 2-simplex if they are connected to each other by edges of length less than or equal to the given threshold. Note that, when the full complex is constructed, it is possible to use homology based tools to compute the number of distinct shape features within the complex.

4.2 Analysis of the Resulting Topological Invariants

Our ultimate tamper/morphing detection would be based on a supervised machine learning scheme that would be trained with a set of sequences, output from the previous step, computed for the Rips simplicial complexes of uniform 2-ones LBP point sets extracted from a set of original and morphed images. Note that, for each image there would be 8-sequences of invariants each representing one of 2-ones LBP rotations. For our proof of concept experiments, we adopted a simplified classification model by confining our analysis to the second entry (i.e. cc_2) of the sequences rather than all the entries. This will allow us to build a simple similarity function and a naive classifier for each of the 8 rotation and then use majority rule at the testing stage. The simple classifier is based on the distributions of the cc_2 values for a training set of original and morphed images.

We trained and tested performance of the classifier(s) using morphed images from the Utrecht face photo database which have been created by [5]. The training was based on, 28 images (14 original and 14 morphed) for each morphing schemes, and calculated the averages and standard deviations of the cc_2 values in each class for each of the 8 rotations of the uniform 2-ones LBP point set. Table 1, below, displays the results obtained for the original images and the 3 morphing schemes.

Table 1. Statistics of connected components (14 original and 14 morphed) images for 2-ones LBP at T_2

LBP code	Original		Splicing morphed		Combined morph		Complete morph	
	Mean	Std.	Mean	Std.	Mean	Std.	Mean	Std.
00000011	16.23	14.19	60.13	13.33	66.83	5.91	31.58	8.94
00000110	20.31	14.62	57.73	14.47	61.83	6.48	36.83	10.58
00001100	21.92	16.63	64.27	13.07	68	4.67	38.75	8.87
00011000	22.31	13.18	65.87	12.68	69	7.32	41.08	8.66
00110000	24	15.80	60.4	10.50	69.58	4.50	37.92	11.60
01100000	22.86	17.90	60.6	11.91	73.58	7.43	37.08	9.01
11000000	18.66	13.97	61.8	10.77	64.42	6.84	35.58	5.93
10000001	22.46	16.87	62.67	11.62	69.42	6.39	38.08	10

The results in this table, show that across all rotations the average cc_2 values for the original images are well below those calculated for the morphed images. Taking into account the corresponding standard deviations, we see that the best separation gap is achieved by the combined morphing scheme followed by those achieved by the splicing morphing, and the complete morphing resulted in significantly lower gaps. The positions of the considered texture features of 2-ones LBP pixels in human face images do not vary significantly, for a proof of concept it is reasonable to suppose that the cc_2 values are normally distributed. At later stages of this research work more sophisticated statistical measures will be used and larger number of images needs to be tested to determine the actual distribution of the cc_2 values.

The above assumption, although not completely necessary, allows us to use known facts about normal distributions to determine with good accuracy the probability that an input image belongs to either class (genuine or morphed). In fact, for each rotation we can classify an input image we simply need to find the position of its cc_2 value in relation to the overlap regions between the two distributions as depicted in Fig. 4.

When classifying any input image, we use all eight rotations and use majority voting to make the final decision on the class of image. Whenever the result of voting was a draw of 4 then it is an 'undecided' case.

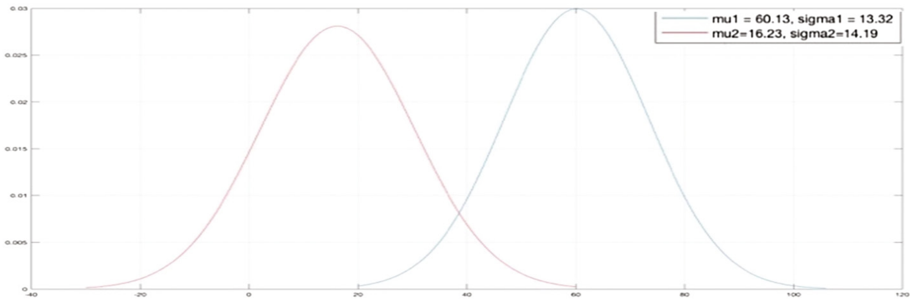

Fig. 4. Distributions of cc_2 values for and the training set of morphed and genuine images

4.3 Testing Experiments

We tested our hypothesis on a large number of face images from the Utrecht face database, excluding the 28 images in the training set. Morphed images in our experiment have been created by Makrushin et al. [5]. We randomly selected 100 images (38 original and 62 morphed) and calculated the cc_2 values for the 8 rotations of the 2-ones LBP pixels and classified them as describe above. For splicing morphing scheme, our method correctly classified 98% of the images. Incorrectly classified images were original images in this case. In the case of combined morph approach, 99% of the input testing images were correctly classified and unlike the splicing technique, misclassified images were morphed images. Unfortunately, around 60% accuracy was achieved with the complete morphing scheme and most misclassified images are morph images.

These testing results, demonstrates the viability of using TDA based classification to automatically detect morphing attacks. More testing are needed to confirm these results and other invariants might have to be incorporated to get high accuracy rates for all existing morphing schemes.

5 Conclusion

We introduced a new topological data analysis based approach to investigate image tampering and in particular to detect known morphing attacks on passport face photo images. The idea was conceived as a result of observations made on a variety of changes in image texture as a result of morphing two original images, and the growing evidence of success of the TDA concept of persistent homology on classification and clustering of textured geometric shapes. We noted a variety of changes of topological invariants of threshold dependent simplicial complexes constructed for uniform LBP image pixel points as a result of morphing. We conducted a proof of concept experiment to test the viability of using TDA for detecting image tampering, and we conclude that the noted changes on the various topological invariants is rich potential of using TDA for the detection of image tampering and to build digital forensics tools. The significantly high accuracy, albeit of limited experimental work, of a morphing detection scheme that uses only the invariance of connected components, as a face related texture descriptor, has shown the potential for success of TDA based approach beyond any doubts.

The next step in this work would be to consolidate our investigations by conducting a much wider experimental work to test and prove the validity of the proposed innovative hypothesis exploiting the huge potential offered by a variety of persistent homology invariants for a mix of different groups of uniform LBP point sets as well as other image texture descriptors.

Acknowledgement. Authors would like to thank Dr. Andrey Makrushin for providing morph images and discussions about morph techniques.

References

1. Ferrara, M., Franco, A., Maltoni, D.: The magic passport. In: IEEE Joint International Conference on Biometrics, Florida (2014)
2. GIMP, GNU Image Manipulation Program. https://www.gimp.org/. Accessed 8 May 2017
3. GIMP, GIMP Animation Package. https://www.gimp.org/tutorials/Using_GAP/. Accessed 8 May 2017
4. Ferrara, M., Franco, A., Maltoni, D.: On the effects of image alterations on face recognition accuracy. In: Bourlai, T. (ed.) Face Recognition Across the Imaging Spectrum, pp. 195–222. Springer, Cham (2016). doi:10.1007/978-3-319-28501-6_9
5. Makrushin, A., Neubert, T., Dittmann, J.: Automatic generation and detection of visually faultless facial morphs. In: Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, Porto (2017)
6. Wang, J., Cha, B., Cho, S., Jay Kuo, C.-C.: Understanding Benford's Law and its vulnerability in image forensics. In: IEEE International Conference on Multimedia and Expo, New York, USA (2009)
7. Gunnar, C.: Topology and data. Bull. Am. Math. Soc. **46**(2), 255–308 (2009)
8. Lum, P., Singh, G., Lehman, A., Ishkanov, T., Vejdemo-Johansson, M., Alagappan, M., Carlsson, J., Carlsson, G.: Extracting insights from the shape of complex data using topology. Nature scientific reports, no. 1236 (2013)
9. Lamar-León, J., García-Reyes, E.B., Gonzalez-Diaz, R.: Human gait identification using persistent homology. In: Alvarez, L., Mejail, M., Gomez, L., Jacobo, J. (eds.) CIARP 2012. LNCS, vol. 7441, pp. 244–251. Springer, Heidelberg (2012). doi:10.1007/978-3-642-33275-3_30
10. Leon, J.L., Alonso, R., Reyes, E.G., Diaz, R.G.: Topological features for monitoring human activities at distance. In: Mazzeo, P.L., Spagnolo, P., Moeslund, T.B. (eds.) AMMDS 2014. LNCS, vol. 8703, pp. 40–51. Springer, Cham (2014). doi:10.1007/978-3-319-13323-2_4
11. Sreeparna, B.: Size functions in galaxy morphology classification. Int. J. Comput. Appl. **100**(3), 1–4 (2014)
12. Rieck, B., Leitte, H.: Persistent homology for the evaluation of dimensionality reduction schemes. In: Eurographics Conference on Visualization (EuroVis) (2015)
13. Janusch, I., Kropatsch, W.: Shape classification using LBP and persistent of critical points. In: International Conference on Discrete Geometry for Computer Imagery, Heidelberg (2016)
14. Edelsbrunner, H., Morozov, D.: Persistent homology: theory and practice. In: European Congress of Mathematics, Kraków, 2–7 July 2012
15. Ojala, T., Pietikainen, M., Harwood, D.: A comparative study of texture measures with classification based on featured distributions. Pattern Recogn. **29**(1), 51–59 (1996)
16. Ahonen, T., Hadid, A., Peitikainen, M.: Face description with local binary patterns: application to face recognition. IEEE Trans. Pattern Anal. Mach. Intell. **28**(12), 2037–2041 (2006)
17. Shan, C., Gong, S., McOwan, P.: Facial expression recognition based on local binary patterns: a comprehensive study. Image Vis. Comput. **27**, 803–816 (2009)
18. Meng, J., Gao, Y., Wang, X., Lin, T., Zhang, J.: Face recognition based on local binary patterns with threshold. In: IEEE International Conference on Granular Computing, pp. 352–356 (2010)
19. Ghrist, R.: Barcodes: the persistent topology of data. Bull. Am. Math. Soc. (New Ser.) **45**(1), 61–75 (2008)

20. Bendich, P., Marron, J., Miller, E., Pieloch, A., Skwerer, S.: Persistent homology analysis of brain artery trees. Ann. Appl. Stat. **10**(1), 198–218 (2016)
21. Rubin, A., Carlsson, G.: Classification of hepatic lesions using the matching metric. Comput. Vis. Image Underst. **121**, 36–42 (2014)
22. Leon, J.L., Cerri, A., Reyes, E.G., Diaz, R.G.: Gait-based gender classification using persistent homology. In: Ruiz-Shulcloper, J., Sanniti di Baja, G. (eds.) CIARP 2013, Part II. LNCS, vol. 8259, pp. 366–373. Springer, Heidelberg (2013). doi:10.1007/978-3-642-41827-3_46