Automatic Detection of Image Morphing by Topology-based Analysis

Sabah Jassim and Aras Asaad
The University of Buckingham, Buckingham, MK18 1EG, UK
{sabah.jassim; aras.asaad}@buckingham.ac.uk

ABSTRACT

Topological Data Analysis (TDA) is an emerging framework for the understanding of Bigdata. This paper investigates and develops a TDA approach to image forensics that exploits the sensitivity to image tampering of a variety of persistent homological invariants of simplicial complexes constructed for certain automatically computed image texture landmarks. For each image, we construct sequences of simplicial complexes, whose vertices are the selected set of landmarks, for a sequence of distance thresholds and use a variety of homological invariants (e.g. number of connected components) to distinguish natural face images from morphed ones. We shall demonstrate the richness of TDA in dealing with image tampering by testing the performance of this approach on a large benchmark image dataset of passport photos in detecting various known morphing attacks.

Keywords — Image Morphing attacks; TDA; Simplicial Complexes; Local Binary Pattern; Persistent Homology.

1. INTRODUCTION

Face biometric is a natural tool for identification tasks such as in law enforcement, border control, surveillance, user identification/verification in mobile phones and many more. Morphing of face images has a serious adverse impact on increasing deployments of automatic border control (ABC) systems [1]. ABC systems incorporate electronic machine readable travel documents (eMRTD) such as e-passport [2]. E-passports incorporates a scanned-printed face photo of the holder and ABC systems compare that with a fresh digital face image as the only biometric reference for verification. Therefore, morphing attacks on face biometric recognition systems gained more attention in the last few years [1], [3]. When a morphed image stored in eMRTD database is similar enough to two persons, then both persons can pass ABC face recognition systems successfully [4]. Ferrara et al., [1], confirmed the failure of 3 automatic face recognition (AFR) systems to differentiate morphed from genuine images. Failure of human experts to differentiate genuine from morphed images was confirmed in [5] and [6].

Morphed images need to be visually faultless and pass ABC systems for both source persons. Advanced techniques have been developed to produce morphed face images, but the *complete*, the *splice* and the *combined* morphing attacks are the most well-known and robust techniques. Complete morphing warps and blends the entire image whereas splicing processes the cropped face region in the image. Thus, complete morphed images have spurious shadows, while splice-based morphed images suffer from minor ghosting artefacts and don't perform well against face recognition. Both schemes depend on the skin color of the two persons. The combined morphing scheme was proposed, in [7], to overcome all these limitations by using the average geometry and texture from both source images.

Many morph detection/prevention schemes have been developed, recently, that deploy known digital forensic approaches that rely on the presence of digital image features that are sensitive to "invisible" changes resulting from morphing, (e.g. [3], [4], [5], and [8]). Most features of interest are naturally linked to image texture landmarks or their statistics. In this paper we extend our pilot study, in [9], and present an innovative topology-based morph detection tool. Our TDA-based approach relies on the availability of a much richer pool of information about morph sensitive texture features than that offered by their mere location/statistics. The topological pool of information, consists of a variety of topological invariants to be computed from a series of simplicial complexes constructed, over a sequences of distance thresholds, from the morph-sensitive texture-based image landmarks. We demonstrate that our topology-based tool outperforms existing morph detection schemes for the above 3 morphing attacks and is robust against print-scan attack. Genuine images used to produce morphed images are available publicly from Utrecht database [10].

The rest of the paper is organised as follows: Section 2 discusses related work, Section 3 introduces the topological image analysis and discuss its suitability for image analysis. In section 4 we describe the TDA morph detector and present experimental results. Section 5 states conclusions.

2. RELATED WORK

Many approaches proposed to detect morphed face images in the last three years after Ferrera et al. in [1] illustrated

ISBN 978-90-827970-1-5 © EURASIP 2018

that morphed face images can bypass all integrity and authentication (optical and electronic) checks. This alarming failure of AFR, motivated research into designing and testing morph detection/prevention schemes.

Raghavendra et al. in [4] proposed a morph detector model based on micro-texture variation using binarized statistical image features. Makrushin et al. in [7] proposed an approach to detect morphed faces based on Benford features of quantized discrete cosine transform of JPEG compressed images. Benford's law states that leading digits of naturally generated random data have a logarithmic distribution. Morphed images are artificially created and seem to violate Benford's law. Hildebrandt et al. in [11] investigated the influence of different image post-processing approaches (e.g. additive noise, scaling and rotation) on the Makrushin et al morph detector using anti-forensic methods, such as StirTrace, and reported that StirTrace processing has a significant impact on morphing detection. In particular, they concluded that adding noise will result in morphed images to be classified as genuine ones. Tom Neubert in [12] presented a progressive image degradation effect, mainly JPEG compression, to discriminate legitimate face images from morphed ones, and concluded that JPEG compression strongly affects genuine images but not morphed images. In [13] deep learning approach to face morphing detection was analyzed using different network architectures.

When it comes to morph detection in print-scanned scenario, to the best of our knowledge the only technique dealing with print-scanned scenario is [8] and [3]. Because the process of printing and scanning digital images may result in losing low-level information, this makes the previous algorithms less effective [14]. Raghavendra et al. in [8] presented an approach based on pre-trained Deep Convolutional Neural Networks (D-CNN) to detect morphed face images. Nonetheless, they reported a significant performance decrease in the case of print-scanned morphed face images. In the same vein, Ferrara et al. in [3] reported that when blending factor is 0.45, their technique significantly increased the morph detection ratio in comparison with results in [8]. Differentiating legitimate face images from morphed ones remains an open issue.

Ferrara et al. [3], proposed a face de-morphing model to be used on a live face image captured at border gates to reveal the genuine passport owner, [3]. The authors examined the effect of the alpha blending factor on detection and concluded that the best blending factor does not exceed 0.3.

3. TOPOLOGICAL IMAGE ANALYSIS

Data analysis in any domain aims to discover patterns in the data representations of the domain objects that can be used for various tasks e.g. classification and recognition. Records are modelled by specific features that are deemed to be discriminating in terms of a specific distance/similarity function. Traditionally, the analysis relies on the extracted features and the pairwise symmetry relations among the data points. Recent big data applications reveal that data is more complex, noisier, has more missing information but more interestingly has shape [15]. Topology is the field of mathematics that studies connectivity and closeness properties of shapes (objects). Topological spaces and their properties are invariant under deformation, coordinate free and can be expressed in a compressed form [16]. The recent emerging paradigm that utilizes the use of topological invariants to understand high dimensional and complex data sets for complex classification applications is known as Topological Data Analysis (TDA). TDA application scope is growing fast and it is out of the scope of this paper to discuss it, however, the recent survey by Massimo Ferri [17] contain a detailed up-to-date applications where topology plays a vital role.

For image analysis, our pilot work in [9] demonstrated that the spatial distribution of landmarks of certain texture features in each image conveys a plethora of topological information, beyond their mere values, which adds a significant discriminating parameters. TDA-based image analysis is akin to a multi-resolution analysis of the shape generated by the image landmarks with respect to a series of thresholding pairwise landmark distances. Extracting insights from images using topological methods has great benefits to machine learning in Image analysis.

Algebraic topology research provides perfect realizations of a multi-resolution topological image analysis scheme via a combinatorial process that yields a series of *Simplicial Complexes* (SC). We use what is known as Vietoris-Rips (Rips for short) simplicial complex construction. Rips complex construction, roughly, is the process of using a set of extracted landmark points as the initial set of 0-dimensional simplices, from which we construct for each distance threshold the set of 1-D simplices (edges of length smaller than the threshold), a set 2-D simplices (triangles from the constructed edges) and 3-D simplices (made up of 4 of the constructed 2-D simplices that have shared nodes) and so on. The simplicial complex shape is made by gluing these simplices together along their edges and faces.

Homology is the most commonly used machinery to characterize topological features/invariants of the Rips SC of shapes. In particular, the properties of homology groups of SC's are used to classify the topology of shapes. For example, the Betti numbers B_n (i.e. the ranks of the n-th homology group of the SC), determines the maximum number of cuts without disconnecting the SC, [18]. The B_0, is the number of connected components (cc) and is widely used for its ease of computing. Instead of depending on the topological invariants at a given threshold, TDA relies more on capturing variation/persistency of these invariants across an increasing sequence of thresholds. In the literature, this is known as persistent homology based analysis, (e.g. [15], [19]). Next we describe our morph detection model.

ISBN 978-90-827970-1-5 © EURASIP 2018

4. TOPOLOGICAL MORPH DETECTOR

First step in designing a topological morph detector is the selection of an appropriate set of automatically extractable image landmarks that are sensitive to morphing. The tool then is construct a sequence of Rips SC's, whose 0-simplices are the landmark pixels, for a finite increasing sequence of thresholds $\{t_i\}$, that ends when the resulting SC is connected. Here, we use different sets of LBP points.

4.1 Local Binary Pattern (LBP).

LBP was originally proposed by Ojala et al. [20] to characterize texture in images. In general, each pixel in the input image will be relabeled by a decimal number that encapsulate the local texture information around it. The LBP process start by subtracting center pixel from its 8-neighbor pixel surrounding it. Starting from top-left corner neighbor, each position will be assigned by 1 or 0 depending on the subtraction result based on the following condition:

$$LBP(x_c, y_c) = \sum_{n=0}^{n=7} s(i_n - i_c)2^n \qquad (1)$$

Where n scans neighbors of the central pixel, i_c and i_n are grayscale values of the central pixel and its surrounding pixels, and the function s(x) is defined as:

$$s(x) = \begin{cases} 1 & if\ x \geq 0 \\ 0 & if\ x < 0 \end{cases} \qquad (2)$$

Each pixel in the resulting LBP image is encoded as a byte determined by the 8 s-bits in a counterclockwise order starting from the top-left corner. An LBP code byte is called uniform if it has 0 or 2 bitwise transitions from 0 to 1. It has been shown that in face images uniform LBP (ULBP) codes constitute 90% of the LBP codes [21]. Therefore, here we opt for choosing sets of uniform LBP points to construct our sequence of Rips SCs. Besides the 2 LBP codes of all 0's and all 1's, there are 56 different ULBP codes that can be split into 7 groups (of 8 codes) each is identified in terms of the number of 1's. Each of these groups is associated with a specific types of image texture. We shall refer to the ULBP bytes that has t consecutive 1's as the t-geometry. We tested the sets of pixels in all the geometries as potential landmarks candidates, and we found, in our pilot study, [9], that all are sensitive to morphing but the 2-ones geometry (representing end line texture) is the most sensitive to morphing.

4.2 Rips Simplicial Complex Construction

Note that each t-ones code is obtained from the byte that has 1 in its t left most position by circular rotation and thus each group subdivides into 8 codes identified by its rotation. Given the positions of the 8 sets of t-ones LBP codes, we proceed to construct 8 sequences of threshold-dependent Rips complexes, one for each rotation of the t-ones codes, using the Euclidian distances. Threshold 0, yield 8 SC's that only consist of 0-simplices, one for each rotation. For simplicity, one can first create a distance matrix D for each rotation before applying other thresholds. The choice of the subsequent thresholds can be determined by subdividing the range of D-values, but we use a fixed sequence of thresholds ($T_1 = 0$, $T_2 = 3$, $T_3 = 5$, $T_4 = 7$, $T_5 = 10$, and $T_6 = 15$). Beyond a certain threshold the simplicial complexes get nearer to become complete graphs which means invariants like the one we use here (No. of connected components) become less discriminating images of different types.

For each rotation, the Rips complexes R_{Ti} constructed over the T_i thresholds i=1 2,..,6, form a nested sequence of SCs:

$$R_{T1} \subseteq R_{T2} \subseteq R_{T3} \subseteq R_{T4} \subseteq R_{T5} \subseteq R_{T6} \qquad (3).$$

For each one of these Rips SC, at a given threshold, distinct homology invariants across the 8 rotations can be used as 8-dimensional feature vectors representing the input image. Here, we use the number of connected components as our Genuine Vs morphed discriminating feature. Figure 1, below, is a block diagram of our topological morph detector.

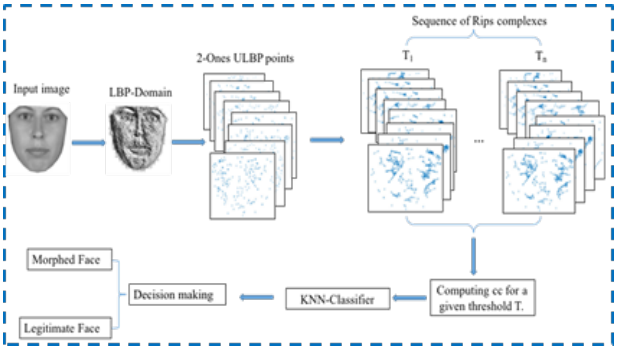

Figure 1: Topological Morph Detector Pipeline.

4.3 Morphing Classification Experiments

Our morph detection tool is based on supervised machine learning using an appropriate classifier at each of the 6 thresholds. Since, our chosen feature vector is of the relatively low dimension of 8 then we opted for the known Nearest Neighbors (KNN, with K=1) [22]. The KNN is a non-parametric, instance based, simple yet robust classifier that uses proximity to template feature vectors of known class selected at the training stage. Our experiments are based on a dataset of thousands of face images formed by applying the 3 morphing, discussed in section 1, using pairs of 71 genuine non-smile images in Utrecht face Database. The dataset of face images used in our experiments consists of: 71 non-smiling genuine face images; 1298 complete morphed images; 2612 splicing morph images; and 2650 combined morph images. All images are segmented such that only the frontal face region will be used to extract ULBP codes using *dlib* library version 19.2 (http://dlib.net/).

The experiments below are restricted to the SCs for 2-ones geometry, and use 4 different evaluation protocols:

ISBN 978-90-827970-1-5 © EURASIP 2018

- P1: Leave-one-out, where one image is randomly selected for testing and the rest are used for training.
- P2, P3 and P4: Respectively 30%, 50% and 70% images are used for training and the rest for testing.

We repeated each experiment 100 times in what is known as 100-fold cross validations. The tables below, show the average detection accuracy for the 3 morphing attacks.

Table 1: KNN Classification for Morphing Attacks.

	Distance Thresholds						
Morphing Schemes	Protocols	T=0	T=3	T=5	T=7	T=10	T=15
Combine Morph	P1	99	99	97	95	98	99
	P2	99	98	97	95	98	99
	P3	99	98	97	95	98	99
	P4	99	98	97	95	98	99
Splicing Morph	P1	97	97	96	100	94	97
	P2	99	97	96	99	94	97
	P3	97	97	96	99	94	97
	P4	97	97	96	99	94	97
Complete Morph	P1	96	96	95	95	92	93
	P2	96	96	95	94	92	93
	P3	96	96	95	94	92	93
	P4	96	96	95	94	92	93

The above table clearly demonstrates significant sensitivity of the cc_2 features to the above morphing schemes at a range of thresholds. Interestingly, accuracy is independent of training protocols. Further analysis of these results, not shown here due to space limitation, show that the false rejection rates are very low ($\approx$ 0.25%) while the false acceptance rates are quite high ($\approx$ 17%). This could be partially due to the imbalanced training which include much larger examples of morphed images than genuine ones. Performance of TDA with other t-ones geometries, have slightly different proportions of errors and fusing several geometries is expected to improve the false positive rates.

We also conducted a limited test of the performance of our approach to detect morphing of print-scanned P&S images. In this test we used 140 images (71 original images, 71 splicing morphed images) printed and then scanned with CanoScan model 9000F MarkII. The images were produced by the Advanced Multimedia and Security Lab (AMSL), Otto-von-Guericke-University of Magdeburg. These images were of different resolutions ranging from 121x136 to 2017 x2517. We rescaled all images into 220x270, extracted the 2-ones ULBP pixels, and constructed their Rips complexes at different thresholds for the 8 rotations as we discussed previously. As before, we extracted the 8-dimensional cc_2 feature vectors at each threshold. The performance of our scheme at the 6-different thresholds are shown in Table 4.

Table 2: NN classification results for P&S Morphing Attack.

	T=0	T=3	T=5	T=7	T=10	T=15
P1	78.87	77.46	73.94	77.46	82.39	72.53
P2	75.64	74.72	74.77	77.1	79.33	70.13
P3	77.97	76.14	74.81	78.28	80.11	72.65
P4	78.57	77	74.76	78.59	81.40	72.38

Although, these results are sufficient to demonstrate the success of TDA approach, they are not as good as their non-print-scanned versions. This may be attributed partly to the significant variation in the image resolution and the fact that the P&S process may result in different level of degrading as a result of using different scanners. Perhaps, the rescaling process have led to variable loss of information. At this stage we cannot compare our P&S results with the techniques in [8] and [3] as they used different scanners. We expect that improved results can be achieved if P&S process use a fixed image size.

These results may seem to be too good to believe, and doubts may be raised about achieving such results for larger datasets of images. To demonstrate that these results are not a case chance, we conducted an experiment on 10,000 natural images randomly selected from the BOSSBase image database (http://dde.binghamton.edu/download/) to test the sensitivity of ULBP codes to tampering. We calculated the number of pixels that are different from their immediate neighbors by ± 1, to estimate the chance that LBP codes changing their structures so that some ULBPs loose their uniform structure while non-uniform LBPs become uniform. Our experiment, revealed that on average more than 78% of the pixels in those natural images have ± 1 differences from their neighbors and thus we expect that reasonable number of changes to number of ULBPs as a result of tampering. This is a good indication of the sensitivity of ULBPs (as well as their sequences of Rips SCs) to morphing as well as to other image tampering.

What makes the proposed tool so powerful is that no prior knowledge about the morphed image is required, and the landmarks are automatically determined. The cc_2 invariant captures the global information of the shape of constructed Rips complexes over different thresholds. These are by no mean the only features that we found to be sensitive to morphing and general image tampering. Indeed, our ongoing research reveal a significant improvement on these results can be achieved by other topological parameters.

5. CONCLUSION

We investigated and developed a novel automatic topological invariant approach to detect morphed face images. Experimental investigations presented in this work demonstrated that morphing process changes the topological

ISBN 978-90-827970-1-5 © EURASIP 2018

properties of the various threshold-based Rips SC's built on certain ULBP landmark points. The excellent classification accuracy that resulted from the connected components feature associated with a single geometry, confirm the success of TDA as a new morph detector which depends on topological properties of constructed shapes from the given photo ID faces. More experiments are needed to improve P&S images classification accuracy. We also need to expand this work beyond the cc feature by including other topological invariants of the Rips SC's. In fact, we have evidences that TDA-based schemes that use other local image information have more potentials for success. Our ongoing work indicate, beyond any doubt, the success of TDA for detecting other tampering attacks.

Acknowledgement. Authors would like to thank all members of Prof Jana Dittmann's research team at AMSL lab of university of Magdeburg for providing Digital and P&S segmented face images as well as various discussions.

REFERENCES

[1] M. Ferrara, A. Franco, and D. Maltoni, "The magic passport," in *IEEE International Joint Conference on Biometrics*, 2014, pp. 1–7.

[2] International Air Transport Association, "IATA - Automated Border Control Implementation." [Online]. Available: http://www.iata.org/whatwedo/passenger/Pages/automated-border-control.aspx. [Accessed: 11-Jan-2018].

[3] M. Ferrara, A. Franco, and D. Maltoni, "Face Demorphing," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 4, pp. 1008–1017, Apr. 2018.

[4] R. Raghavendra, K. B. Raja, and C. Busch, "Detecting morphed face images," in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems, BTAS 2016*, 2016.

[5] D. J. Robertson, R. S. S. Kramer, and A. M. Burton, "Fraudulent ID using face morphs: Experiments on human and automatic recognition," *PLoS One*, vol. 12, no. 3, 2017.

[6] M. Ferrara, A. Franco, and D. Maltoni, "On the effects of image alterations on face recognition accuracy," in *Face Recognition Across the Imaging Spectrum*, 2016, pp. 195–222.

[7] A. Makrushin, T. Neubert, and J. Dittmann, "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*, 2017, pp. 39–50.

[8] R. Raghavendra, K. B. Raja, S. Venkatesh, and C. Busch, "Transferable Deep-CNN Features for Detecting Digital and Print-Scanned Morphed Face Images," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2017, vol. 2017–July, pp. 1822–1830.

[9] A. Asaad and S. Jassim, *Topological Data Analysis for image tampering detection*, vol. 10431 LNCS. 2017.

[10] P. Hancock, "Psychological Image Collection at Stirling (PICS)-2D face sets," *Utrecht ECVP http://pics.stir.ac.uk/2D_face_sets.htm*. [Online]. Available: http://pics.stir.ac.uk/2D_face_sets.htm. [Accessed: 17-Jan-2018].

[11] M. Hildebrandt, T. Neubert, A. Makrushin, and J. Dittmann, "Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps," in *Proceedings - 2017 5th International Workshop on Biometrics and Forensics, IWBF 2017*, 2017.

[12] T. Neubert, "Face Morphing Detection: An Approach Based on Image Degradation Analysis," Springer, Cham, 2017, pp. 93–106.

[13] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert, "Detection of Face Morphing Attacks by Deep Learning," Springer, Cham, 2017, pp. 107–120.

[14] U. Scherhag, R. Raghavendra, K. B. Raja, M. Gomez-Barrero, C. Rathgeb, and C. Busch, "On the vulnerability of face recognition systems towards morphed face attacks," in *Proceedings - 2017 5th International Workshop on Biometrics and Forensics, IWBF 2017*, 2017.

[15] G. Carlsson, "TOPOLOGY AND DATA," *Bull. New. Ser. Am. Math. Soc.*, vol. 46, no. 209, pp. 255–308, 2009.

[16] P. Y. Lum *et al.*, "Extracting insights from the shape of complex data using topology," *Sci. Rep.*, vol. 3, no. 1, p. 1236, Dec. 2013.

[17] M. Ferri, "Persistent topology for natural data analysis — A survey," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10344 LNAI, pp. 117–133.

[18] M. Gardner, *Martin Gardner's Sixth book of mathematical diversions from Scientific American.* University of Chicago Press, 1983.

[19] R. Ghrist, "Barcodes: The persistent topology of data," in *Bulletin of the American Mathematical Society*, 2008, vol. 45, no. 1, pp. 61–75.

[20] T. Ojala, M. Pietikäinen, and D. Harwood, "A comparative study of texture measures with classification based on featured distributions," *Pattern Recognit.*, vol. 29, no. 1, pp. 51–59, Jan. 1996.

[21] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 7, pp. 971–987, Jul. 2002.

[22] T. Cover and P. Hart, "Nearest neighbor pattern classification," *IEEE Trans. Inf. Theory*, vol. 13, no. 1, pp. 21–27, Jan. 1967.