Digital Signal Processing 23 (2013) 1505–1522

Contents lists available at SciVerse ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Key-dependent 3D model hashing for authentication using heat kernel signature

Suk-Hwan Lee [a,*], Ki-Ryong Kwon [b], Won-Joo Hwang [c], V. Chandrasekar [d]

[a] Department of Information Security, Tongmyong University, 535, Yongdang-Dong, Namgu, Busan, 608-711, Republic of Korea
[b] Division of IT Convergence and Application Engineering, Pukyong National University, 599-1, Daeyeon-Dong, Namgu, Busan, 608-739, Republic of Korea
[c] Department of Information and Communications System, UHRC, Inje University, Gimhae, Geyongnam, Republic of Korea
[d] Electrical and Computer Engineering Department, Colorado State University, Fort Collins, CO 80523, USA

ARTICLE INFO

Article history:
Available online 7 May 2013

Keywords:
3D model hashing
Heat kernel signature
Authentication
Copy detection
Multimedia security

ABSTRACT

Multimedia-based hashing is considered an important technique for achieving authentication and copy detection in digital contents. However, 3D model hashing has not been as widely used as image or video hashing. In this study, we develop a robust 3D mesh-model hashing scheme based on a heat kernel signature (HKS) that can describe a multi-scale shape curve and is robust against isometric modifications. We further discuss the robustness, uniqueness, security, and spaciousness of the method for 3D model hashing. In the proposed hashing scheme, we calculate the local and global HKS coefficients of vertices through time scales and 2D cell coefficients by clustering HKS coefficients with variable bin sizes based on an estimated L^2 risk function, and generate the binary hash through binarization of the intermediate hash values by combining the cell values and the random values. In addition, we use two parameters, bin center points and cell amplitudes, which are obtained through an iterative refinement process, to improve the robustness, uniqueness, security, and spaciousness further, and combine them in a hash with a key. By evaluating the robustness, uniqueness, and spaciousness experimentally, and through a security analysis based on the differential entropy, we verify that our hashing scheme outperforms conventional hashing schemes.

1. Introduction

Recently, multimedia security has become a very important issue. It has been said that the authentication and identification of multimedia to ensure trustworthiness will be important in the future, because new paradigms based on pre-pay or auxiliary pay models will be developed [1]. Traditionally, the authentication and identification of a message are addressed by cryptographic hashes, which are key-dependent and sensitive to bit alteration. However, this is no longer a suitable way to authenticate multimedia data since it allows content-preserved attacks, and therefore an authentication tool that validates multimedia data is more desirable. Studies have been conducted to find a multimedia-based hash that is insensitive to bit alteration but does not cause quality degradation, i.e., a content-based digital signature of the multimedia media data. Multimedia data undergo various manipulations such as compression and enhancement. A multimedia-based hash thus takes into account changes in the visual domain.

A number of media-specific hash functions have been proposed for multimedia authentication [2–8]. However, most multimedia-based hashing methods focus on images and video. Swaminathan et al. [2] presented a random key-dependent image hashing method using Fourier–Mellin transform coefficients. This method is robust against RST (Rotation, Scaling, and Translation) and filtering; the security evaluation of the image hash is based on differential entropy. Mao et al. [3] analyzed the security of an image hash using the unicity distance proposed by Shannon. Monga et al. presented a robust image hashing method based on non-negative matrix factorization [4], end-stopped wavelet transformation using FDoG (Flow-based Difference of Gaussians) and Morlet wavelets [5], and random clustering [6]. Coskun et al. [7] presented a video hashing method using temporal and spatial transform coefficients based on 3D-DCT (Discrete Cosine Transform) and 3D-RBT (Randomized Basis Set). De Roover et al. [8] presented a video hashing method using a RASH (Radial hASHing) vector of keyframes in a video sequence. In addition to these, many other methods for image and video based hashing have been proposed.

With the rapid growth of the 3D content markets, 3D model hashing has become a necessity for authentication and copy detection. Currently 3D model hashing is receiving less attention than have 3D watermarking [9–17], 3D retrieval [18–24], 3D segmentation [25–28], and shape matching [29–31]. Image hashing methods

* Corresponding author. Fax: +82 51 628 1129.
E-mail addresses: skylee@tu.ac.kr, sukhwanlee@gmail.com (S.-H. Lee), krkwon@pknu.ac.kr, kiryongkwon@gmail.com (K.-R. Kwon), ichwang@inje.ac.kr (W.-J. Hwang), chandra@engr.colostate.edu (V. Chandrasekar).

1051-2004/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.dsp.2013.04.012

cannot be applied to 3D models because they are based on popular polygonal or curve modeling methods, unlike images, which are based on pixels. Likewise, 3D model hashing cannot be applied to images or video, taking over image/video hashing, because the content-based hashing depends on the structure of the media data. 3D model hashing can be used as a core technique for 3D security of authentication, forensics, and copy detection. Furthermore, it can be applied in a number of 3D industry fields, such as movies (CG, animation), game content, drawing/mapping (3D GIS, 3D CAD), medical models, and content libraries.

The desired properties of 3D model hashing are *robustness*, *uniqueness*, *security*, and *spaciousness*, which are similar to those of image hashing [2–8]. *Robustness* means that a hash should be insensitive to perceptual modifications caused by 3D editing operations. *Uniqueness* means that hashes are statistically independent for both different models with the same keys and different keys in the same model. *Security* means that it should be difficult to detect a hash from a model without knowing the key. Since hash in an attacked model may be identified falsely as any hash of another model, an additional desirable property of 3D model hashing is that attacked hashes should be statistically independent of each other. This property is an extension of the robustness and uniqueness properties between which there is a trade-off relationship. *Spaciousness* means that the perceptual space of a model is sufficiently large and also a model in this space shares a hash. In order to achieve the above properties, many image-hashing methods are based on a key-dependent hash function.

The few studies that have been reported to date include Hamza et al.'s on the information-theoretic hashing of a 3D mesh using spectral graph theory and entropic spanning trees [32,33]. This scheme applies Eigen-decomposition to the Laplace–Beltrami matrix of each sub-mesh, and then generates the hash value based on the spectral coefficients and the Tsallis entropy estimate. A hash value is a real number and the length of a hash is dependent on the number of sub-meshes. Formerly, M. Reuter et al. [29,30] used the Laplace–Beltrami spectra as fingerprints or shape-DNAs for geometric invariants. They defined and proved the isometry and scaling invariant, similarity, efficiency, compression, and physicality of shape-DNA, and applied shape-DNA for shape discrimination, retrieval, and matching. Thus, shape-DNA may be used as shape features in applications in copyright protection, retrieval, shape matching, and quality assessment. The above two methods do not satisfy the properties of security and spaciousness because they generate a real hash value that depends on the model shape without randomization or a security key. Therefore, in the strict sense, they do not address 3D model hashing for authentication and copy detection purposes.

Lee et al. [34,35] presented a robust 3D mesh hashing based on a key-dependent 3D surface feature, namely, the block shape feature that combines the curvedness [25] and the shape index [20–22]. This scheme exhibits robustness against some attacks, including the uniqueness of the model and key, and security. However, it cannot be robust against the mesh simplification and tessellation of topologic attacks.

Naturally, the feature vector is an important factor in hashing, as well as in watermarking, retrieval, segmentation, and shape matching. Recently, benchmark results for the performance of shape feature detectors and descriptors were reported in [36,37]. The authors evaluated feature detection and feature description methods separately by applying transformations: isometry, topology, hole, scaling, noise, and down-sampling. The evaluated feature detection methods belong to three families: heat kernel-based features [38], 3D Harris features [39], and salient points [40]. Similarly, the evaluated feature description methods belong to three families: heat kernel signature [38], dense heat kernel signature [23,24], and spin image signatures [41]. This report indicated that, on average, the heat kernel-based feature and heat kernel signature (HKS) perform best in experiments that address robustness. The main advantage of HKS is that it is an isometry-invariant multi-scale feature that can capture information about neighborhoods of a given point, and is stable under shape perturbations [38]. Raviv et al. [42] presented a volumetric HKS, the so-called VHKS, for robust isometry invariant volumetric descriptors. They reported that VHKS is more robust under strong isometric and topological transformations and is less sensitive to noise and resampling; however, VHKS is not scale-invariant and its complexity is greater than that of HKS [38]. In addition, they reported that, while both VHKS and HKS are capable of discriminating between non-isometric shapes, HKS is invariant under volume-changing isometries of the boundary, whereas VHKS is not. From these results, it can be seen that HKS may be beneficial for the robust feature of the intermediate hash vectors.

There is some analogy between hash functions and shape feature/signatures: both can be used for copyright protection, retrieval, and watermarking. However, a hash function has to achieve copy detection, authentication, and security, unlike a shape feature/signature.

This paper presents a method of 3D model hashing for authentication and copy detection, not a shape feature and signature. In this paper, we discuss the properties related to the *robustness*, *uniqueness*, *security*, and *spaciousness* of 3D model hashing, and we then propose an HKS-based 3D model hashing scheme that is dependent on a key and parameters, which satisfies the four properties. The four properties are important requirements for achieving copy detection and authentication of a 3D model. The proposed hashing obtains HKSs at multiple scales on the mesh surface and generates a binary hash through the feature extraction from HKSs that depends on a key and parameter refinement. We compute HKSs at each vertex on a mesh by eigenvalues and eigenvectors of a mesh Laplace operator [38] that is estimated discretely from the Laplace–Beltrami operator. We use two parameters to improve the four properties further. The first parameter is related to the uniqueness and security of the key. The second parameter is related to robustness. Two parameters are finally reset through an iterative refinement process to improve the *spaciousness* and *uniqueness* among hashes in all models with different keys and in the same model with different keys.

We evaluated the robustness against various geometric and topologic attacks using a public 3D editing tool, and we evaluated the uniqueness of the models and keys and the spaciousness by measuring the attack intensity in the available authentication range. These properties were evaluated according to the normalized Hamming distance. Lastly, we evaluated the security by modeling the differential entropy of the intermediate hash according to Swaminathan et al.'s method [2]. Experimental results verified that, for all requirements, the proposed hashing performance is superior to that of conventional hashing.

The rest of the paper is organized as follows. In Section 2, we introduce the structure of a content hashing method that focuses on the 3D model. Then, we present an HKS-based 3D mesh hashing that is dependent on a key and parameters, in Section 3. In Section 4, we discuss the evaluation of the robustness, spaciousness, uniqueness, and security of the proposed hashing. Finally, we draw conclusions and describe our future research, in Section 5.

2. Related works

In this section, we introduce the general concept and requirements of a 3D model hashing based on the framework of image hashing presented by Swaminathan et al. [2] and Monga et al. [4–6], and the theory of the heat kernel signature for feature vectors [38].