This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2010 proceedings

A Proposed Digital Rights Management System for 3D Graphics using Biometric Watermarks

Rakhi C. Motwani*, Frederick C. Harris, Jr.* and Kostas E. Bekris*
*Department of Computer Science and Engineering
University of Nevada, Reno USA 89507

***Abstract*—This paper proposes a new DRM system for 3D graphics that makes use of biometric watermarking technology. The presented solution utilizes an image of a biometric trait e.g. face or fingerprint, and embeds it into the 3D graphics as a watermark. This biometric watermark is then used to authenticate a legitimate user. Details for the components of the DRM framework are presented. Adoption of biometric watermarking allows the DRM system to provide consumers unrestricted access to the graphics along with limiting graphics content access to only legitimate users, thereby protecting artists from large scale online piracy. A detailed survey of existing DRM solutions for 3D graphics is provided to identify the limitations of each implementation which offers either restrictive content usage scenarios or is ineffective in preventing unauthorized usage.**

I. Introduction

The diverse applications of 3D graphics ranging from the entertainment industry to the commercial domain, scientific world, computer aided design and much more have given rise to online warehouses that sell 3D models. However, once a 3D model is sold it can be illegally redistributed to users who have not paid to own the graphic. Digital rights management (DRM) solutions are designed to address such piracy issues. A review of existing DRM systems for 3D graphics content reveals that these systems either offer restrictive usage scenarios to deter piracy or offer unrestrictive usage but are unable to prevent piracy. This paper proposes a novel biometric-watermarking based DRM system that allows consumers to use 3D graphics without any restrictions and deters large scale online piracy.

Watermarking techniques have been used for copyright protection of digital media and use data hiding technology to encode small information into digital content with no perceivable difference. Traditional watermarking techniques embed text, unique identifiers, copyright ownership messages, logos, image or digital media content-based information into the multimedia. The proposed system utilizes the biometric data of a consumer as a watermark. Biometric watermarks are preferred over typical IDs because biometrics offer an access control mechanism, and serve as stronger deterrents to piracy. The embedded biometric watermark is used to authenticate a user in order to secure the graphics content from illegitimate access. While a user specific pin or password can be illegally shared by an authorized user with many other users, concerns related to privacy(misuse of one's biometric data) and piracy litigation(since biometric data enables content owners to indisputably identify the source of piracy) discourage an authorized user from sharing biometric data that unlocks illegally redistributed graphics content.

The rest of this paper is organized as follows. Section II reviews DRM implementations for 3D graphics. Section III outlines the proposed DRM system's framework, the functionality of each component, security aspects of the DRM system, and measures for the system's performance. Future work and conclusions are summed up in Section IV.

II. Literature Review

A. 3D Graphics DRM Systems

Published literature related to 3D graphics DRM is very limited. The issues with existing DRM systems that are highlighted in the literature can be summarized as:

- Device-limiting access
- Usage restrictions
- Unauthorized access

Related work on digital rights management of 3D graphics is analyzed based on the type of implementation:

1) Client-Server Based Implementation: Stanford University has signed a contract with the Italian authorities to protect the laser scanned high resolution 3D digital sculptures of Michelangelo by making the artwork available only to established scholars for noncommercial use. The goal of the team [1] that has undertaken the project is to prevent piracy of the 3D models such that simulated marble replicas are not manufactured by unauthorized entities. To achieve this objective, they have implemented a remote-rendering system with client-server architecture that allows interactive display and manipulation of the artwork but provides only low resolution 2D renderings to academic users. To address the analog attack, the authors discourage 3D reconstruction from 2D images by having the server impose constraints on rendering requests, disallowing extremely close-up views of models and requiring a fixed field of view.

This DRM model is geared towards shared content security and counters piracy by restricting what users can do with the graphics. The user, however, can share his login credentials but this kind of dishonesty does not impact the content owner's primary objective of preventing piracy. While this system is not device binding and can be accessed from any machine, it does limit the users' flexibility to use the graphics as the user does not own the content. This system is not designed as a business model to trade, manage, and monitor redistribution of sold content.

978-1-4244-5176-0/10/$26.00 ©2010 IEEE

2) Cryptography and Watermarking-Based Implementation: Sohn *et al.* [2] propose a watermarking based 3D data files security component for an Intelligent Manufacturing System which is used to develop digital prototypes in the manufacturing industry. The objective of this system is to prevent 3D data files from leaking out of the organization. This server-based 3D watermarking system, named as 3DGuard, works according to security policies that define the user's access rights and permissions. A watermarking plug-in intercepts a users upload or download action in order to embed, retrieve, or remove watermarks on 3D files as per security policies stored on server. Every 3D data file has a watermark that is specific to the user who last accessed the file from the system. In case a 3D data file is leaked out of the organization, the source of the leak can be determined by analyzing the user-specific watermark embedded into the file.

Kwon *et al.* [3] present a DRM scheme for 3D animation games serviced in mobile devices. Due to the limited bandwidth and high cost associated with directly downloading game content to a mobile device, game sellers allow consumers to download the game on a PC and then transfer the content to a mobile device. The scheme is designed to prevent illegal redistribution of purchased 3D game content by addressing scenarios where consumers illegally transfer the PC downloaded game content to multiple mobile devices. Authors present a solution that employs the Buyer-Seller watermarking protocol [4] for consumers protection and tracing illegal redistribution. The consumer generates a pair of public and private keys. The public key is circulated to a third-party referred to as the Watermarking Certification authority, who is responsible for generating an encrypted watermark for the buyer. The watermark is then sent to the seller to embed into the game content. The seller inserts a second watermark in the game as well in case the consumer is able to remove the first watermark from the game content. The seller encrypts the game content with the buyer's public key such that the game can only be unlocked by the buyer's private key. This encryption safeguards the consumer from dishonest sellers who may illegally redistribute a buyer's game to other consumers and hold the buyer responsible for piracy. Since the buyer is the only one with access to the private key that decrypts the game content, that game content can not be unlocked by anyone else. Should the buyer share his private key and a pirated copy of the game is found, the seller verifies the unique tracer watermark of each buyer and determines the specified buyer suspected of unauthorized distribution.

These DRM solutions offer consumers full access to content, but the nature of the implementations facilitate users to make illegal copies as well. Therefore, these systems fails to prevent unauthorized distribution and usage. However, these systems do succeed in deterring illegal circulation since consumers are aware of the possibility of being tracked down and held responsible for piracy if the pirated content is found by the owners. The underlying assumption is that the watermark has not been damaged by the consumer to remove traces of his identity from the pirated graphic content. However, in order to make sure the tracer watermark identifies a customer without any disputes, the kind of watermark used should be unique to every customer.

3) Hardware-Based Implementation: Shi *et al.* [5] present a hardware-based digital rights management solution that integrates digital rights functionalities within the Graphics Processing Unit (GPU). Their goal is to counter piracy of real time graphics entertainment software. Authors propose the hardware design and API extensions to integrate cryptography within the GPU. The GPU has two additional components - a cryptographic unit to decrypt graphics data during rendering in real-time, and a license verification unit to process texture and shader binding constraints designated in the licenses of graphics data to circumvent security threats posed by loose coupling of textures and shader programs with geometry data.

Hardware DRM solutions provide a higher level of protection as opposed to software DRM solutions as it is difficult to break the system by software based attacks or by hardware tampering to dump signal traces at chip interconnects. However, hardware systems are not feasible for the consumer market due to cost concerns [6] since appropriate hardware components need to be installed on the consumers computer. Besides, this system is realized on a GPU architecture simulator. Hardware realization of the concept is far from reality yet as the nature of the presented research requires a cross-disciplinary collaboration in digital rights management (DRM) community, graphics researchers, and GPU architects.

III. Proposed Approach

To date there is no published work on using biometrics as watermarks in 3D models within the DRM framework. In this paper, a novel DRM framework is presented which has two stages - i) enrollment and ii) authentication. The consumer provides his biometric images during enrollment, prior to purchasing the graphics. The system inserts the biometric image of the consumer as watermark into the purchased 3D graphics, wraps the watermarked graphic in a custom file format so that the graphic file can not be accessed outside the system, and encrypts these contents using a consumer-specific key. This packaged content is then distributed to the consumer. The primary goal of the custom file format is to enable access control by notifying a graphics consumption application that a file is DRM enabled. The custom file format is a just way to bind the graphics to the DRM system in order to prevent users from bypassing the access control mechanism. The custom file format also assists in content editing, logging, and system renewability. When the consumer attempts to access the graphics file, the authentication stage prompts the consumer to provide his biometric image and compares this newly acquired biometric image with the biometric image embedded as watermark to verify the consumer's legitimacy. Based on the computed similarity measure between the acquired and embedded biometric images, the system authenticates the user to access the graphics. A predefined threshold value is set for the similarity measure to distinguish a genuine user from an illegitimate user. An illegitimate user's biometric provided at

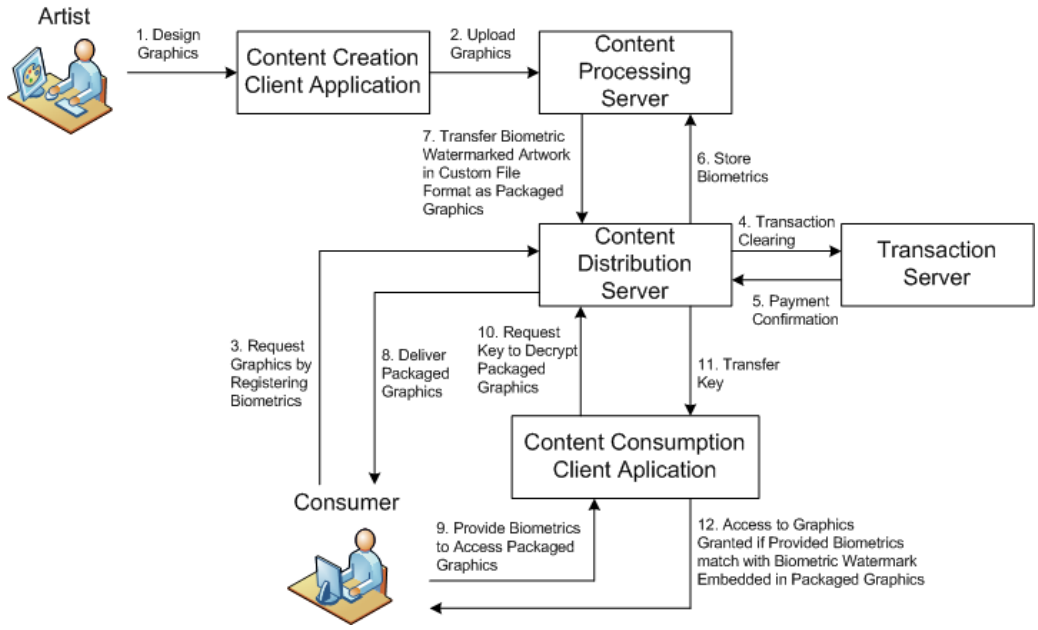

Fig. 1. DRM System Framework

access time does not match with a genuine user's biometric embedded as the watermark, so the system denies access to the graphics.

If the biometric watermark can't be retrieved from the graphic file, the system denies access to the graphic file. Therefore, the system does not rely on the assumption that the biometric watermark is intact and has not been destroyed by hackers. This feature discourages consumers from tampering with the packaged graphics. If illegal copies of the artwork are redistributed by a legitimate user, the biometric watermark travels with the artwork and secures it from illegitimate usage. This is because the custom file format prevents consumers from accessing the file outside the DRM system, and the authentication stage of the system sieves legitimate users from illegitimate users. Therefore, the biometric watermark protects the graphics content from being used by any other than the valid user.

If the system is compromised and the artwork is distributed and accessed by any one other than the legitimate user, the embedded biometric serves as a tracer. The pirated graphic file is examined for the embedded biometric watermark. If the biometric watermark has not been tampered with, it assists in tracing back illegitimate redistribution to the traitor in the distribution chain and suing the responsible for piracy, since every biometric watermark is unique to the consumer. Privacy concerns over sharing one's biometric trait along with the purchased protected graphic content on peer-to-peer(P2P) networks, prevents large scale piracy of the artwork.

In the event of compromised biometrics, since a biometric trait cannot be revoked the framework supports multiple biometrics so the compromised trait is replaced by an alternative trait. Furthermore, upon receiving notification of compromised biometrics from the user, the server deactivates the user-specific key thereby locking out access to files previously encrypted with this key and issues a new key for the user. This new key is used to encrypt files previously purchased by the user, so only the legitimate user is able to access these files in spite of the compromised biometrics.

The process model for the DRM system is outlined in Fig. 1. This framework shows the basic components of the system and the logical work flow from creation to consumption of the graphic file. The system utilizes a client-server protocol for implementation and involves a custom file format that can be interpreted by any graphics design/consumption application that incorporates the proposed DRM system by installing the DRM client in the form of a custom plug-in. The server-side of the system consists of a Content Processing Server, Distribution Server and Transaction Server. The client-side of the system consists of a Content Creation Application and Content Consumption Application.

A. DRM System Components

The proposed DRM system has five components: Content Creation, Content Processing, Transaction Management, Content Distribution, Content Consumption. Functionality of each component is specified below.

1) Content Creation: Artists use a graphics design application to create the artwork. The design software has DRM capabilities after installation of a DRM plug-in that interprets the custom file format used to wrap the graphics content. The plug-in for the artists also include the watermark embedder, detector and matcher components, and an interface to connect to the graphics repository on the Content Server.

2) Content Processing: The user enrollment interfaces provided by the content distribution component acquire and securely transfer the acquired biometric image of the user to

the content server, as outlined in Fig. 2. Due to consumer privacy concerns [7], the biometric image is encrypted and then stored in a repository along with an associated user identifier. The packaging module is responsible for conversion of graphics to custom file format representation. The graphic content is watermarked with an encrypted version of the biometric image. A key is generated for the user, stored in the key repository and linked with the user's identifier. The packager encrypts the content with this key and makes it is ready for distribution to the user in the form of packaged graphics.

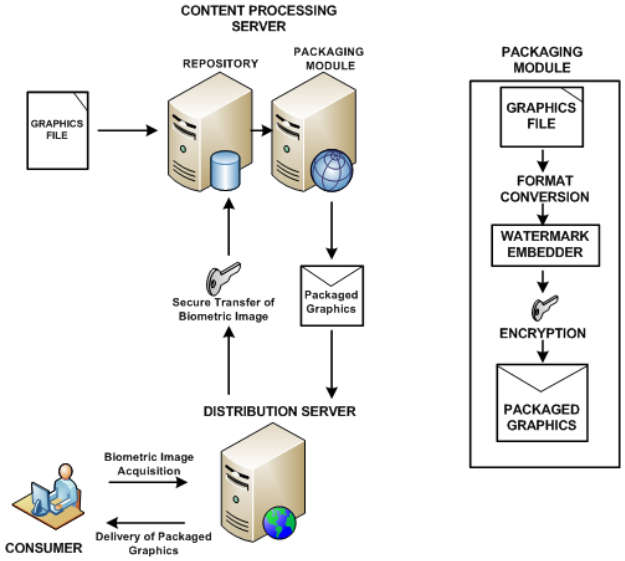

Fig. 2. Content Processing

The watermark embedder normalizes [8] the 3D graphics model, to make the watermarking robust to geometric distortions such as rotation, scaling and translation. The selection of vertices, appropriate for embedding the watermark, is determined by computing the curvature variation of the model at the 1-ring neighborhood of each vertex [9]. The selected vertices are modified by adding the watermark using a scaling factor to ensure minimal perceptual distortion to the model. The indices and original values of the watermarked vertices are stored in the key.

3) Transaction Management: This component handles the user registration, commerce and billing activities. It includes a module for interaction with an external payment service to handle the financial aspects of the purchase transaction. After payment is received, this server sends confirmation to the Distribution Server to release the packaged graphics to the user.

4) Content Distribution: The main function of this component is enrollment of the user and handling trading aspects of the transaction. It maintains a website which provides interfaces to register the user, accept payment information, capture user's biometric images, and securely transfer the acquired information to the Content Processing and Transaction Servers. Distribution of the packaged graphics to the client is also handled by this component. Distribution is carried out over a secure transmission channel.

5) Content Consumption: The client-side DRM enabled graphics consumption application is responsible for authorizing rightful users to access the purchased graphics. The DRM plug-in installed at the client application will have the watermark extractor and matcher component, as portrayed in Fig. 3. When an attempt is made to access the file by the end user, the 3D content consumption application prompts the consumer to provide his/her biometric image. The plug-in sends the server the user's identifier(a biometric hash or pre-assigned username) to request the key to decrypt the graphics file contents. The watermark extractor component normalizes the 3D model and then utilizes the key to retrieve the embedded watermark. The matcher component generates a biometric template from the extracted watermark i.e. biometric image, compares it to the biometric template generated from the acquired biometric image to validate legitimacy of the user. A match between the two biometric templates grants access to the user, while a mismatch locks down the graphic file. Biometric templates match only if their computed similarity measure is greater than a predefined threshold. If the watermark extractor is unable to retrieve the watermark from the graphics, the system denies access to the file.

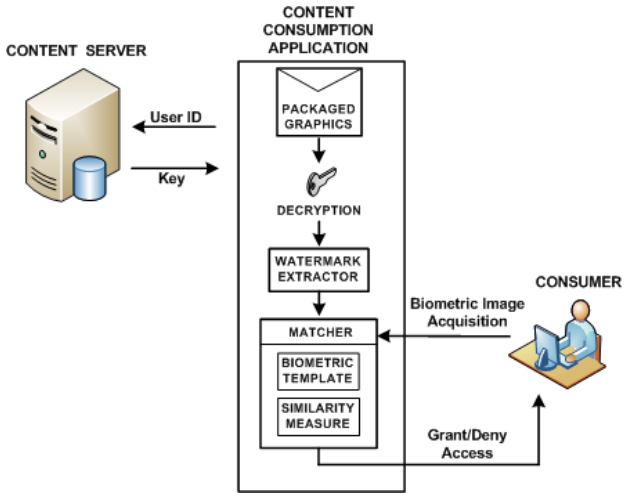

Fig. 3. Content Consumption

During registration when the user is enrolled into the system, the user is given the option to provide images of his/her face, fingerprint, or both biometric traits. If the user opted to provide a face image, the matcher component is configured to formulate a biometric template(face print) from the face image.

Face print generation process has 3 modules as illustrated in Fig. 4: face detection/localization, face normalization and feature extraction. The face region is localized [10] from the input image, and is normalized using photometric normalization algorithm [11] such that the resultant image is invariant to illumination conditions at the time of image capture. Normalization step loses some details but preserves

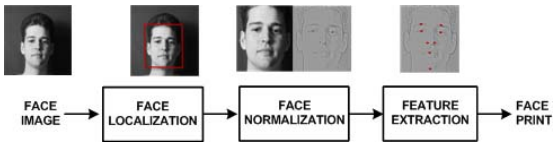

Fig. 4. Face Print Generation

the main features such as eyes, mouth and nose along with the distance proportion. Eyebrow, eye, nose, mouth, and chin features are located using techniques suggested by [12]. The generated face print is a description of the distance between these facial feature points. The matcher component correlates the face prints using a Euclidean distance measure.

In the case of fingerprint biometric template generation [13], a preprocessing stage segments and enhances the fingerprint portion of the image, as shown in Fig. 5. Fingerprint patterns such as loops, whorls, arches, ridges, and furrows are extracted as features from the processed fingerprint image, to constitute the biometric template. The matcher uses correlation based technique [14] to compute similarity between the biometric templates of the acquired fingerprint image and the embedded fingerprint image.

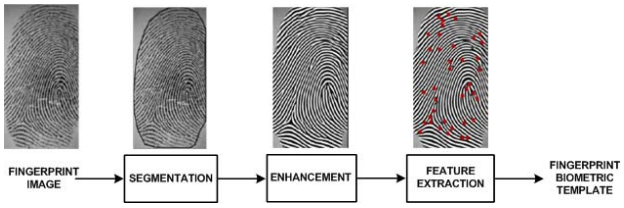

Fig. 5. Fingerprint Biometric Template Generation [Fingerprint Images taken from *Handbook of Biometrics* [13]]

The plug-in provides access management by tracking *save as, modify and save, cut, copy, paste, print screen* operations on the graphics file. It keeps track of the user activity in regards to modifying and copying the graphics to new files and updates the header of the custom file format with appropriate logging information. This logging assists the plug-in to maintain the presence of the biometric watermark in the graphics content regardless of modifying or saving of the graphics to a new file.

B. System Performance

Accuracy of the matcher component depends on the biometric trait used, representation scheme used to extract and model the relevant features from the captured biometric trait, and the similarity measures used for comparison of the user's biometric trait. The performance of any biometric-based system is measured in terms of the False Acceptance rate (FA) and the False Rejection (FR) rate. False acceptance is the case where an illegitimate user is granted access by the system. False rejection is the case where a genuine user is denied access by the system. The robustness of the system is based on this performance characterization of biometrics. Since user adoption of such a DRM system is the biggest challenge, it is best to use biometrics with low FA and FR rates. Face has a false reject rate of 4% and false accept rate of 10% while fingerprints have a false reject and accept rate of 2%, as cited in [15]. The proposed system would have similar results since the implementation will be based upon the best algorithms for the selected biometric. To further improve the accuracy of the system, fusion of other biometrics such as hand, voice, and signature with face or fingerprint can be considered.

C. Security Aspects of the DRM System

The goal of an adversary is to try to break the security of the system in order to obtain the graphics content in an unprotected form. Therefore, it is necessary to build a security model [16] that states the security goals of the system along with identifying all possible means by which an adversary can attempt to attack the system. The primary security goal of this DRM system is to prevent illegitimate access to the legally distributed 3D graphics. The secondary goal of the system is to trace illegally accessible graphics back to the buyer responsible for unauthorized redistribution.

According to Kerckhoff's principle, the strength of a system should lie entirely in the difficulty in determining the key and not in the secrecy of the algorithm. The proposed system utilizes a consumer-specific key to encrypt/decrypt the custom file format. The custom file format merely serves as a container for the raw graphics data and the purpose of the key is to make it difficult for the adversary to segregate this raw graphics data that is wrapped in the custom file format. The system is breached if this key is accessible to the adversary, for the unprotected graphics data can be separated from the decrypted custom file format. Furthermore, the watermarked graphics are vulnerable to various attacks [17] that may lead to destruction or removal of the biometric watermark disabling the system from tracing the origin of piracy. Therefore, the system completely relies on the secure storage of this key in order to protect the data.

The security assumption made by the system is that the communication between the artist, the DRM client and servers, and the consumer takes place through a secure channel in order to protect information from eavesdropping when it is transmitted. The system is subject to various threats at the server and client side of the application. The Content Server is prone to hacking. An adversary can exploit security flaws in the server to obtain control over any one of the server repositories(that store the biometric templates, keys and unpackaged graphics) and the packaging module to defeat the system. The adversary has complete control over the user side consumption application and can replace the watermark extractor or matcher component. The user-specific key acquired from the server is temporarily stored on the client's machine and is vulnerable to exposure. Attacks against the graphics rendering application can replace part of the rendering application to capture and save decrypted graphics. If the user's biometric trait is compromised (i.e. an adversary obtains the biometric of a legitimate user without his consent or knowledge), the

adversary fraudulently gains access to the protected graphics file with the legitimate biometric trait.

IV. Conclusions And Future work

This paper presents a novel approach to address the problem of piracy by employing a biometric watermarking scheme and proposes a DRM framework that offers - i) content access to a legitimate user, ii) device portability, iii) restriction-free usage to consumers, iv) eliminates the traditional use of licenses to govern the usage of the content, and v) deters piracy to protect artists and artwork sellers from incurring losses. The proposed DRM system can be adapted to support different digital content types such as documents, images, audio and video.

The proposed technique is superior to a biometric authentication system [18] that could utilize a unique ID watermark for tracing, because biometric-based sign-on procedure authenticates a user to gain access to the system, subsequently enabling an authorized user to copy the content out of the system and illegally redistribute it. In such cases, the unique ID watermark serves as a means to identify the user responsible for piracy. However, if such a system were to employ a custom file format, illegitimate users could not gain access to the system to consume the content without having access to the biometrics of the authorized user, so piracy would still be deterred but legitimate users would be restricted to that particular system and would not enjoy the feature of interoperability.

To the contrary, even though the proposed approach utilizes a custom file format encrypted by a key, it supports interoperability because the custom format only serves as a container for the watermarked graphics in order to enforce access control. The watermarked graphics can be in any format. The custom format can be interpreted by any 3D graphics software that has the DRM client installed. In case of piracy, the biometric watermark travels with the graphics file and secures the graphics from illegitimate access. The pirated graphics file is accessible to the illegitimate user only if the authorized user who has leaked the graphics content, supplements the contents with his biometric data.

If the key is compromised and the contents of the custom file format are decrypted, the access control mechanism is defeated and the biometric watermark serves as a tracer. While the biometric watermark and the unique ID both serve as tracers that assist in identifying the individual responsible for piracy, a biometric watermark serves as a stronger deterrent to piracy than a unique ID. This is because biometrics are a personal trait which not only give away the identity of the user (such as face, fingerprint images) but can also be potentially misused by illegitimate users. To the contrary, there are no such privacy issues associated with a unique ID-based watermark, since the scope of a unique ID is just limited to the context of the application. By making use of biometric data as a watermark, the proposed approach benefits in two ways - authentication and tracing, wherein lies the novelty of the approach.

Future work involves incorporating behavioral biometrics such as voice and a handwritten signature to safeguard the system from the use of substitutes e.g. legitimate user's face and fingerprint images shared with unauthorized users to circumvent the system's biometrics validation phase. By use of voice or handwritten signature, the system can dynamically prompt the user to speak or hand write random text phrases at access time to circumvent the use of substitute biometrics. Accuracy of the system can be improved through the use of multi-modal biometrics such as fusion of face and voice. The system currently supports only personal use of files and must be extended to feature multiple users in a corporate environment. The system design can also be revised to embed a biometric template as opposed to a biometric image.

References

[1] D. Koller and M. Levoy, "Protecting 3D graphics content," *Commun. ACM*, vol. 48, no. 6, pp. 74–80, 2005.

[2] Y. Sohn, G. Wallmann, and M. Fernandes, "User transparent 3D watermarking system based on security policy," in *International Conference on Cyberworlds*, Oct. 2007, pp. 89–92.

[3] S.-G. Kwon, S.-H. Lee, K.-R. Kwon, E.-J. Lee, S.-Y. Ok, and S.-H. Bae, "Mobile 3D game contents watermarking based on buyer-seller watermarking protocol," *IEICE - Trans. Inf. Syst.*, vol. E91-D, no. 7, pp. 2018–2026, 2008.

[4] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Transactions on Image Processing*, vol. 10, no. 4, pp. 643–649, Apr 2001.

[5] W. Shi, H. Lee, R. Yoo, and A. Boldyreva, "A digital rights enabled graphics processing system," in *Proceedings of the 21st ACM SIGGRAPH/EUROGRAPHICS Symposium on Graphics Hardware*, 2006, pp. 17–26.

[6] H. Federrath, "Scientific evaluation of DRM systems," in *Konferenz Digital Rights Management*, 2002. [Online]. Available: http://epub.uni-regensburg.de/7502/

[7] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal of Advanced Signal Processing*, pp. 1–17, 2008.

[8] W. Liu and S. Sun, "Rotation, scaling and translation invariant blind digital watermarking for 3D mesh models," in *First International Conference on Innovative Computing, Information and Control*, vol. 3, 2006, pp. 463–466.

[9] R. C. Motwani and F. C. Harris, "Robust 3d watermarking using vertex smoothness measure," in *Proceedings of the International Conference on Image Processing, Computer Vision, and Pattern Recognition*, July 2009.

[10] J.-W. Wang, "Face localization in cluttered background," in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Aug. 2008, pp. 585–589.

[11] J. Short, J. Kittler, and K. Messer, "A comparison of photometric normalisation algorithms for face verification," in *Proceedings. Sixth IEEE International Conference on Automatic Face and Gesture Recognition*, May 2004, pp. 254–259.

[12] S. Tsekeridou and I. Pitas, "Facial feature extraction in frontal views using biometric analogies," in *Proceedings of EUSIPCO*, 1998, pp. 315–318.

[13] A. Jain, P. Flynn, and A. Ross, *Handbook of Biometrics*. Springer-Verlag New York, Inc., 2007.

[14] A. Cavusoglu and S. Gorgunoglu, "A robust correlation based fingerprint matching algorithm for verification," *Journal of Applied Sciences*, vol. 7, no. 21, pp. 3286–3291, 2007.

[15] A. Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross, "Biometrics: a grand challenge," in *Proceedings of the 17th International Conference on Pattern Recognition*, vol. 2, Aug. 2004, pp. 935–942.

[16] H. Jonker, S. Mauw, J. Verschuren, and A. Schoonen, "Security aspects of DRM systems," in *25th Symposium on Information Theory in The Benelux*, 2004, pp. 169–176.

[17] I. Cox, M. Miller, and J. Bloom, *Digital watermarking*. Morgan Kaufmann, 2002.

[18] J. Ortega-Garcia, J. Bigun, D. Reynolds, and J. Gonzalez-Rodriguez, "Authentication gets personal with biometrics," *Signal Processing Magazine, IEEE*, vol. 21, no. 2, pp. 50–62, Mar 2004.