Parity enhanced topology based spot area watermarking method for copyright protection of layered 3D triangular mesh data

Md. Mahfuzur Rahman1[†] *and Koichi Harada2*[††]*,*

Department of Information Engineering, Hiroshima University, Japan.

Summary
A parity enhanced topology based spot area watermarking method is proposed to embed information in objects with layered 3D triangular meshes such as those reconstructed from CT or MRI data. With the integration of parity checking, it improves the robustness against unauthorized alteration of a single bit in every consecutive 8-bits of length. Watermark message is cut into several pieces and each piece of message is embedded at different spots so that if a piece of message is lost in one spot, the same information can be potentially retrieved from other spots by error correct decoding. The method compares height of the vertices of a triangle lying in the same layer. A watermark message is converted into a binary bit sequence, a parity bit is added with every consecutive 8 bits, and then embedded into the model in either way that the first vertex of a triangle in the upper level or in the lower level, that carries information 1 or 0, respectively. For experimental purpose, a watermark message is embedded in a mouse embryo model. It is robust against translation, rotation, arbitrary re-sectioning, local deformation, scaling, and unauthorized alteration of a single bit in every consequent 8-bits length. It is useful for shape sensitive 3D geometric models. It left some artifacts after re-arrangement of local or global numbering. These artifacts have vertices sorted in descending order in terms of degree. These unique features can also be used for 3D data retrieval.

Key words:
Watermarking, layered 3D triangular mesh model, topology based embedding, computer graphics, copyright protection.

Introduction

In digital media environment, it is very easy to copy, modify and distribute various kinds of digital data such as texts, images, audios, videos and recently 3D geometric models through Internet, CD-ROM, etc. In this environment an important research is watermarking of these data for Intellectual property protection as well as for efficient data management and content labeling. The bulk of the research of watermarking of digital media has focused on media such as texts, images, videos, and audios [1, 2]. Recently 3D geometric models have been widely used in the area of CAD, CAM and Computer Graphics as well as in medical applications and have been recognized as important models. Telemedicine, robot assisted operation, virtual operation, etc. are very promising future trend of research in medical science where there is a lot of use of reconstructed 3D geometric models of different objects. So, watermarking of these 3D geometric models is very important in these days.

Geometry, topology and attributes can be a target of embedding watermark in 3D geometrical models. Researchers have mainly focused on embedding watermark in the geometry of a 3D model [3, 6, 8, 11, 12, 13, 14], while a few have targeted parametric curves and surfaces [10]. Others have targeted movement of 3D models, that is, MPEG4 facial animation parameters [5] or attributes of 3D models. R. Ohbuchi, et al. presented some idea about topology based watermarking of 3D models [9]. However, 3D geometric models, such as for medical applications, rarely tolerate its changes in geometry i.e. they are geometry sensitive and they often subject to arbitrary re-sectioning. This ultimately indicates the importance of effective topology based watermarking method resistant to arbitrary re-sectioning.

Generally 3D model, which consists of polygons, has geometrical values that are the coordinates of vertices and topology (connectivity) among them. This paper's contribution is in topology based watermarking of 3D triangular mesh model. Parity checking is normally used in signal processing and so far my knowledge goes it is not used in watermarking methods. However, it can improve the robustness of the method against unauthorized alteration of a single bit in a consecutive 8-bits length. Here a parity enhanced topology based watermarking method is proposed to embed information in objects with layered 3D triangular meshes such as those reconstructed from CT or MRI data. Watermark message is cut into several pieces and each piece of message is embedded at different spots so that if a piece of message is lost in one spot, the same message can be potentially retrieved from other spot by error correct decoding. These spots are uniquely determined.

Manuscript received February 25, 2006.
Manuscript revised February 28 , 2006.

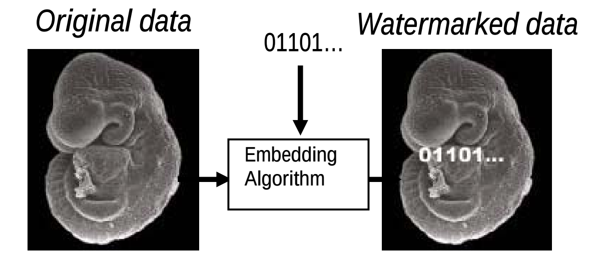


Fig. 1 (a): Watermark embedding process

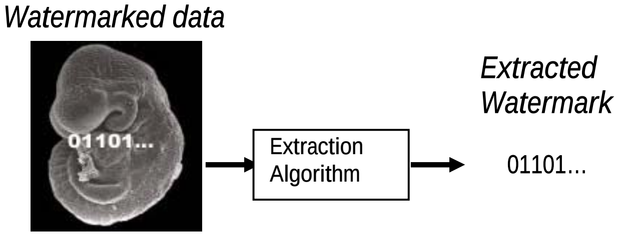


Fig. 1 (b): Watermark extraction process

It utilizes the redundancy of topological information as well as the layered structure of the model to embed data into it. Embedding and extraction of watermark are done successfully. It is fast, efficient and effective. It is invisible and robust against translation, rotation, scaling and arbitrary re-sectioning. It is useful for content labeling, ownership data assertion, efficient data management, detection of change of data etc. prevailing the way for copyright protection of precious 3D model data.

Watermarking loosely refers to the use of steganography in the application areas of ownership assertion, authentication, content leveling, content protection, distribution channel tracing etc. while steganography addresses the problem of hiding information within digital data. In watermarking process, an invisible digital watermark such as important data identification information, copyright or ownership data is embedded into the original data. Then, the author distributes this watermarked data instead of the original data. When necessary, the author can extract the embedded watermark by using the appropriate extraction algorithm. The process is shown in Fig. 1. Not only copyright protection, identification of important data i.e. content labeling, efficient data management as well as detection of change of data are also important roles of watermarking.

.

2. Background and main idea

Layered data is commonly used in medical field. In medical applications there are many 3D triangular mesh models reconstructed from CT (Computer Tomography), MRI (Magnetic Resonance Imaging) data which are having layered construction. However, these models, used for medical applications, are very sensitive to geometrical error and often subject to arbitrary re-sectioning for application purpose. So, topology based arbitrary re-section resistant algorithm is necessary to watermark these models. We found that it is possible to exploit the layered construction as well as the irregular triangulation of these models to embed data into it topologically making it arbitrary re-sectioning resistant.

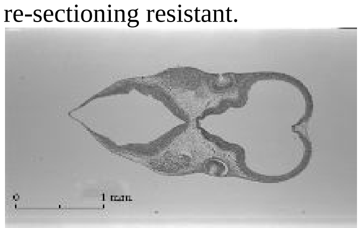


Fig. 2(a): Mouse Embryo cross-section

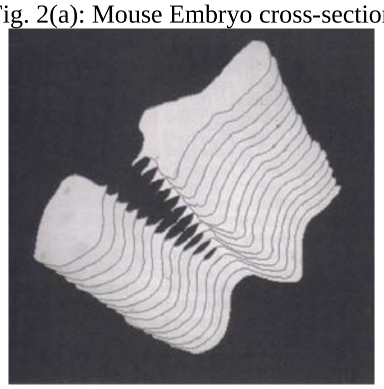


Fig. 2(b): Stack of extracted parallel contours

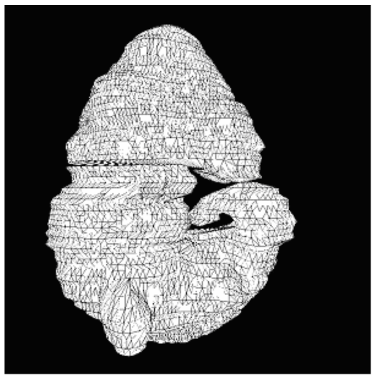


Fig.2(c): Reconstructed mouse embryo model

A mouse embryo model [4] is used, as an example, to embed a watermark. The model is reconstructed from serial sections taken from an optical microscope. One such section is shown in Fig. 2 (a). Sections are further processed and finally they become digital picture elements, the pixels. Contour-based reconstruction is used for surface formation of the model. In contour-based reconstruction the idea is to compute the structure boundary in each individual slice as contour lines and to estimate the 3D boundary surfaces as a set of patching elements (usually triangles) that envelops a given set of contours. These contours are all parallel as shown in Fig. 2(b). Reconstructed mouse embryo model, having layered construction, is shown in Fig. 2(c). The developed method aims at embedding watermark topologically to the layered construction of a model keeping the geometry unchanged making it arbitrary re-section resistant enhanced with parity check. A watermark message is cut into pieces and each piece of message is embedded at different spots so that if a piece of message is missing at one spot, it can be retrieved from other spot by error correct decoding. The algorithm compares height of the vertices of a triangle lying in the same layer. A watermark message is converted into a binary bit sequence, a parity bit is added with every consequent 8-bits, and then embedded into the model in either way that the first vertex of a triangle in the upper level or in the lower level, that carries information 1 or 0, respectively (see Sec. 4). The watermark extraction process is the reverse process of embedding.

3. Requirements of watermarking

The requirements of a watermarking method are always application specific. Still there are some general requirements, what majority of the watermarking methods should satisfy, can be categorized as follows:

1. Perceptually invisibility
   The embedded watermark must be perceptually invisible and unnoticeable for a third party in terms of model's intended use.
2. Capacity of the watermark
   The amount of watermark embedded should be large enough to record important data identification, author's information etc.
3. Robustness
   The embedded watermark should be robust against 3D affine transformations, such as translation, rotation and scaling, which are frequently applied to 3D geometric models. For application purpose the model may need to be cut into several pieces or local deformation could be done to reshape a model. So, the embedding should withstand re-sectioning and local deformation. Some watermarking methods also need to be robust against intentional attacks such as filtering, compression, re-meshing and noise addition to the watermarked model or these operations should degrade the quality of the model regarding its intended use.
4. Geometrical error
   The geometrical error caused by the watermark (if any) should be restricted within the specified tolerance according to the application. However, many of the 3D geometric models are error sensitive and rarely tolerate any error.

4. Parity enhanced spot area algorithm

A watermark message is cut into pieces and each piece of message is embedded at different spots so that if a piece of message is missing at one spot, it can be retrieved from other spot by error correct decoding. Topological information of layered structure of triangular mesh is used to embed watermark. The potential of such layered structure is that as long as layered structure exists, if two of the vertices of a triangle are in the lower level, then the rest vertex will be in the upper level or vice versa. The algorithm compares height of the vertices of a triangle lying in the same layer. A watermark message is converted into a binary bit sequence, a parity bit is added with every consequent 8-bits, and then embedded into the model in either way that the first vertex of a triangle in the upper level or in the lower level, that caries information 1 or 0, respectively. The watermark extraction process is the reverse process of embedding.

Step 1: Preparing binary watermark

It produces a binary representation of a textual watermark message data. Prior to application, the message data are encrypted to an unintelligible format with well-known and powerful RSA encryption algorithm. With every consecutive 8 bits, a parity bit is added to make an even parity.

Step 2: Message package setup (See Fig. 4 (a))

Flag bit is set to 1 to check upside-down rotation. Header stores total bit numbers in a message package and footer stores total bit numbers written in a model.

Flag	Header	Message piece	Footer

Fig. 4 (a): Structure of message package

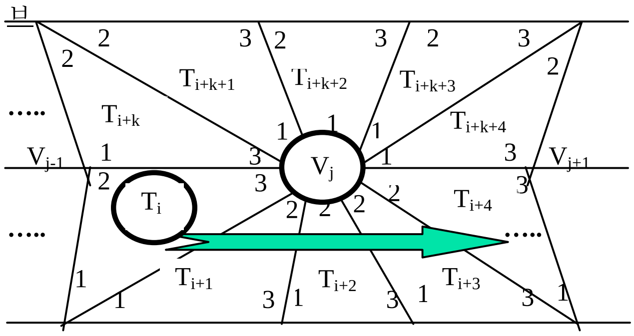


Fig. 4 (b): Starting triangle

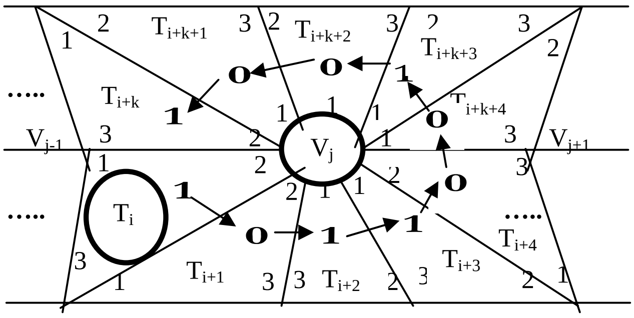


Fig. 4 (c): Embedding a binary sequence "1011001001"

If the model is rotated upside down, the flag bit embedded at the starting point, will be set to 0 and the method will change its extraction strategy. Header is used to determine the end of a message package. Footer is useful for checking whether the watermark is destroyed or not by cut off operation, local deformation, and so on.

Step 3: Selection of the starting point

Because of the nature of an arbitrary tessellation, it is not likely that all the vertices would have same degree. The method first sorts the vertices in descending order depending on its degree. The vertex having the second highest degree (or valence) is found in a triangular mesh model, and the neighbor triangle with the smallest *id* number is decided as the starting triangle. As shown in Fig. 4 (b) vertex V_j possesses second highest degree in a triangular mesh model. Triangle T_i is the smallest in *id* number among neighbor triangles, and hence it is selected as the starting triangle.

Step 4: Data embedding

Message package composed in ***step 2*** is embedded in different spots. These spots are selected based on the lowest *id* neighbor triangle of sorted vertices of ***step 3***.

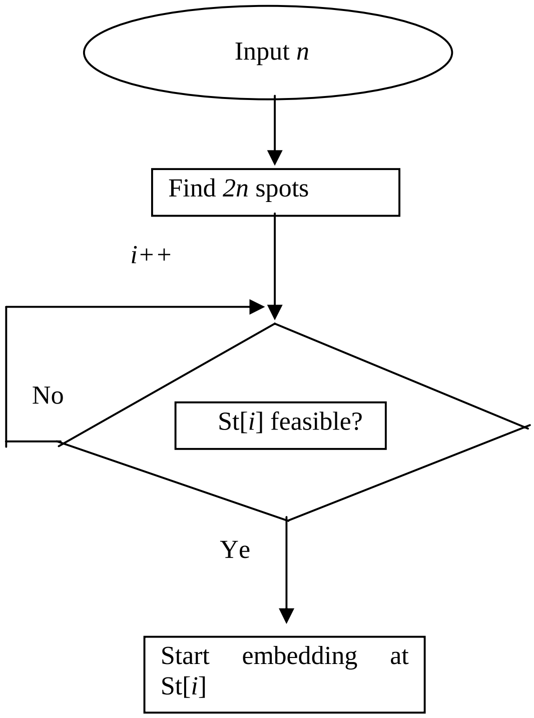


Fig. 4 (d): Flow chart for spot selection

It is shown in Fig. 4 (b). If user selects *n* spots of watermarking, the algorithm first finds out *2n* number of spots and then selects feasible n candidates and hereby embeds the watermark. In flow chart this spot selection part can be illustrated as shown in Fig. 4 (d).

Local numbering of the vertices of a triangle is changed to embed data. The first vertex in the upper and lower levels carries information 1 and 0, respectively. A binary bit pattern "1011001001" is embedded in the mesh as shown in Fig. 4 (c). Embedding starts from starting triangle and goes in circular fashion encircling the vertex. After embedding data in first ring, it continues to embed data in second ring and so on till the end of message package. As the algorithm changes only the local numbering of the triangular patch of the model, the geometry of the model remains totally the same.

Step 5: Data extraction

The extraction process is the reverse process of embedding. Un-watermarked model i.e. the original model is not needed for data extraction and hence it is considered as the public watermarking scheme.

To extract embedded watermark, first of all we check whether the model is rotated with respect to horizontal axis. If rotated, it is rotated back so that the contours are all parallel to the horizontal axis.

Vertices are sorted in the descending order depending on its degree. Vertex having second highest degree is found and hence the neighbor triangle with the smallest *id* is found. This is the starting point of data extraction. In this point it decodes the first bit of information to check flag bit. If flag bit is reset i.e. if the local numbering of the first vertex of the triangle is found in the lower level, we understand that the model is rotated upside down and hence changes extraction strategy considering that local numbering of the first vertex of a triangle in the upper level carries information 0.

From the starting triangle embedded binary information are extracted checking whether the local number of the first vertex of a triangle is in the upper level or in the lower level that carries information 1 and 0, respectively.

The associated spots are selected based on the lowest *id* neighbor triangle of the sorted vertices. If some part of the message is missing in one spot, because of re-sectioning, the same information is retrieved from other spot by error correct decoding.

Header stores total bit numbers in a message package. So, it is used to determine the ending of a message package. Footer stores total bit numbers written in a model. It is useful to check whether any information is lost due to cut – off operation or any extra information is added by a third party.

After retrieving binary information, text data is prepared using reverse process of **Step 1**.

5. Practical application and discussion

In the experiment, following message is embedded in to the mouse embryo model:

“A new topology based watermarking method for layered 3D triangular mesh model developed my Md. Mahfuzur Rahman, Ph.D. student, Media Graphics Lab, Hiroshima University, Japan”.

The message is composed of 177 characters i.e. 1624 bits of information is embedded including 1 bit flag, 10 bits header, 177 bits parity and 20 bits footer.

Watermark is embedded in a mouse embryo model consisting of 61 layers, 3 elements, 15776 vertices, and 31318 triangles. The message package composed of a flag, selector, header, message and footer.

First, following normal triangle numbering, total watermark message is embedded sequentially for four times changing a selected unique starting point. The second, third and other starting points are found in the same way described above. As the same watermark is embedded for four times, the total number of bits written in the model is 6496 bits.

Retrieval of the watermark is also done successfully. Watermarked area of the model is visualized with red colored triangles as shown in fig. 5(a). It is important to mention here that the watermarks are visualized only for the purpose of demonstration. In practical application the watermarks remain totally invisible. The model is composed of 3 elements i.e. three elements are integrated in a single model. Three elements are visualized separately for visualization of all the watermarks. Element 3 is inside element 2, and elements 3 and 2 are inside element 1.


Element 1


Element 2

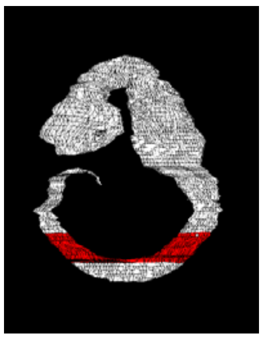
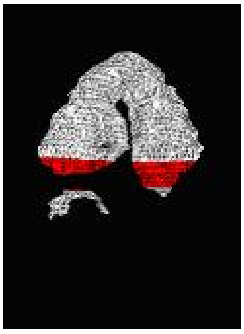

Element 3

Fig. 5(a): Mouse embryo model after embedding

Here, triangles are numbered horizontally. So, horizontal re-sectioning may not destroy all the embedded watermarks but vertical or arbitrary re-sectioning can partially destroy all the four watermarks as shown in Fig. 5(b). and it is the fact that for application purpose such models often subject to arbitrary re-sectioning.

To make the watermark robust against arbitrary re-sectioning, the proposed method cuts the message into small pieces and every piece of information is embedded at several spots as shown in Fig 4 (c). During extraction, if the algorithm finds that a piece of information is lost in one place, it decodes it from other spot using error correct decoding. Here spots are indicated with red colored marks only for demonstration purpose. In practical application, these spots are totally invisible.

Element 1



Element 2

Element 3

Fig. 5 (b): After arbitrary re-sectioning

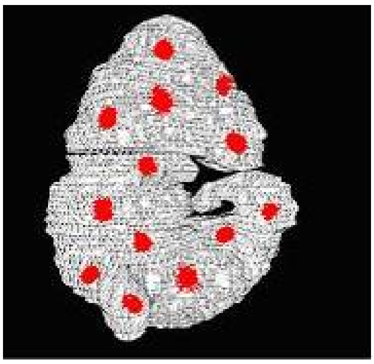


Fig. 5 (c): Parity enhanced spot area embedding

The method is robust against major unintentional attacks such as translation, rotation, scaling, re-sectioning and keep some artifacts even after some intentional attacks such as local number re-arrangement and global number re-arrangement. These artifacts have unique starting points and the number of its associated triangles. From these artifacts the owner of the model can claim its originality. These artifacts are unique to every specific model. It is unlikely that two different models with irregular tessellation will have same artifacts.

With proper knowledge of embedding process, practically every watermark is possible to destroy. In our case if local numbering of the triangles are re-arranged then the embedded watermark will be destroyed but still it lefts some identifying mark i.e. unique starting triangle as well as the vertex connected with maximum number of triangles. These data are unique feature for every specific model. In case of random tessellation of a mesh, it is not likely that all the triangles will have same degree. Practical experiment shows that it varies a lot. Vertices sorted in descending order with respective degree or valance is unique for a specific model. The limitation of this approach is that it is not usable for regular triangular mesh.

As in the first step of the method the bit stream is encrypted to an unintelligible format with famous and powerful RSA encryption algorithm, even if the intruder detects the watermark, the person cannot read it because the message is in encrypted format.

The proposed method fulfills majority of the general watermarking requirements. It is invisible, capacity is high enough and it can withstand translation, rotation and scaling. It is also robust against arbitrary re-sectioning and enhanced with parity check. The method is similar to triangle strip peeling symbol sequence embedding (TSPS) [9], but it is more advantageous as shown in table 1.

Comparison criteria	TSPS [9]	The proposed method
Bounding edge crossing problem	Has problem	No problem
Applicable to data type	Any type of triangular mesh	Only layered triangular mesh
Space efficiency	Lower	Higher
Non- uniform scaling	Not robust	Robust
Starting point	Not uniquely determined and not topological	Uniquely determined and topological

Mesh type	Mesh should be orientable	No such requirements
Arbitrary re-sectioning	Not robust	Robust
Parity check	Not available	Available

Table 1: Comparison with TSPS

6. Conclusions and future works

The proposed method is simple, effective, computationally faster, and inexpensive. It is robust against unintentional attacks translation, rotation, arbitrary re-sectioning, scaling etc. and left artifact after intentional attacks of local and global number re-arrangement. As it is parity enhanced, it can check alteration of a single bit in every consecutive 8-bits length. It is applicable for important data identification, detection of change of data, content labeling, ownership assertion, etc. of layered 3D triangular mesh models. It is very useful for watermarking of geometry sensitive 3D triangular mesh model.

Further extension of the method is possible developing an embedded program that will destroy the model or degrade the quality of the model in-terms of its intended use if re-meshing or mesh simplification is applied to it.

Acknowledgements

The first author would like to thank Japanese Ministry of Education, Science, Sports and Culture as well as “Gakushu Shoreihi” scholarship provider for sponsoring the research work.

References

[1] W. Bender, D. Gruhl, N. Morimoto and A. Lu, Techniques for data hiding, IBM Systems Journal, Vol. 35, Nos. 3&4, pp. 313-336, 1996.

[2] I. J. Cox and M. L. Miller, A review of watermarking and the importance of perceptual modeling, Proc. SPIE Conference on Human Vision and Electronic Imaging II, Vol. 3016, pp. 92-99, February 1997.

[3] O. Benedens, Geometry-Based Watermarking of 3D Models, IEEE CG & A, Vol. 19, No. 1, pp. 46-55, 1999

[4] Roman Durikovic, Kazufumi Kaneda, Hideo Yamashita, Imaging and Modelling from Serial Microscopic Sections for the study of Anatomy, Medical & Biological Engineering & Computing, Vol. 36, No. 3, pp. 276-284, 1998

[5] F. Hartung, P. Eisert and B. Girod, Digital Watermarking of MPEG-4 Facial Animation Parameters, Computer Graphics, Elsevier, Vol. 22, No. 4, pp. 425-435, 1998

[6] S. Kanai, H. Date, and T. Kishinami, Digital Watermarking for 3D Polygons using Multiresolution Wavelet Decomposition, Proc. of the Sixth IFIP WG 5.2 International Workshop on Geometric Modeling : Fundamentals and Applications, pp. 296-307, 1998

[7] S. Katzenbeisser, F. A. P. Petitcolas, Information Hiding, Techniques for steganography and Digital Watermarking, Artech House, London, 2000

[8] R. Ohbuchi, H. Masuda, and M. Aono, Watermarking Three-Dimensional Polygonal Models, Proceedings of the ACM Multimedia `97, Seattle, Washington, USA, pp. 261-272, 1997

[9] R. Ohbuchi, H. Masuda, and M. Aono, Watermarking of 3D Polygonal Models Through Geometric and Topological Modifications, IEEE JSAC, pp. 551-560, 1998.

[10] R. Ohbuchi, et al., A shape-Preserving Data Embedding Algorithm for NURBS Curves and Surfaces, Proc. Computer Graphics International` 99, pp. 177-180, 1999

[11] R. Ohbuchi, A. Mukaiyama, S. Takahashi, A Frequency-Domain Approach to Watermarking 3D Shapes, in Proc. EUROGRAPHICS 2002, September, 2002

[12] Ryutarou Ohbuchi, Hiro Ueda, Shu Endoh, Robust Watermarking of Vector Digital Maps, in proceedings of the *IEEE Conference on Multimedia and Expo 2002 (ICME 2002)*, Lausanne, Switzerland, August 26-29, 2002.

[13] R. Ohbuchi, Akio Mukaiyama, Shigeo Takahashi, Watermarking 3D shape model defined as a point set, Proceedings of the 2004 international conference on cyberworlds, pp. 392-399, 2004.

[14] E. Praun, H. Hoppe and A. Finkelstein, Robust Mesh Watermarking, MSR-TR-99-05, Microsoft Research, SIGGRAPH, 1999.

Acknowledgments

The first author would like to thank Japanese Ministry of Education, Science, Sports and Culture as well as “Gakushu Shoreihi” scholarship provider for sponsoring the research work.

Md. Mahfuzur Rahman received the B.Sc.(Engg.) in Electrical and Electronic Engineering from Khulna University of Engineering and Technology, Bangladesh and the M.Sc. (Engg.) in Computer Science and Enginering from Zhejiang University, China in 1996 and 1999 respectively. During 1999 – 2003 he stayed in Intelligent Systems and Modeling Lab, Hiroshima University, Japan as research scholar supported by Japanese Govt. Monbusho scholarship. Currently he is pursuing his Ph.D. at Media Graphics Lab, Hiroshima University, Japan. He is a member of IEB (Institute of Engineers, Bangladesh), BSC (Bangladesh Computer Society) and a student member of IEEE.

Koichi Harada Ph.D., a professor of Graduate School of Engineering, Department of Information Engineering and the chief of Media Graphics Lab, Hiroshima University, Japan.