International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **3**, March **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 1055–1074

A NOVEL HIGH CAPACITY 3D STEGANOGRAPHIC ALGORITHM

Meng-Tsan Li, Nien-Ching Huang and Chung-Ming Wang*

Institute of Computer Science and Engineering
National Chung Hsing University
No. 250, Kuo Kuang Rd., Taichung 402, Taiwan
{ holylight; phd9005 }@cs.nchu.edu.tw
*Corresponding author: cmwang@cs.nchu.edu.tw

Received October 2009; revised April 2010

Abstract. *This paper presents a powerful high capacity 3D steganographic algorithm which can embed more than 9.6 million bits of a secret message using a 3D polygon model with only 14,004 vertices. To the best of our knowledge, this is the largest capacity ever reported in the literature. We accomplish this novel algorithm by using two levels of message encoding. In the first level, we subdivide the secret message into a number of payload fragments. We then encode each payload fragment by utilizing a corresponding random sample generated on a unit sphere. In the second level, we encode these random samples to a number of feature points which convey the payload fragment and are skillfully located on the surface of an existing 3D polygon model. The procedure produces a point cloud stego model that can be delivered in a public channel for steganographic purposes. We produce dummy points by uniform sampling over the surface area of the 3D polygon model which increases the rendering quality of the point cloud stego model and also prevents suspicion of the messages by eavesdroppers. Our scheme has five features. First, it can embed a significantly large number of payloads using 3D polygonal models with small complexity. Theoretical analysis indicates that our algorithm has a significantly high capacity with the magnitude of 50 bits per feature point, outperforming that offered by the current state-of-the-art 3D steganographic algorithms. Second, the scheme is flexible, allowing it to convey various capacities by adjusting two region partition parameters. Third, it belongs to a distortion-free manner, and encounters no model variation because of the hidden message. Fourth, the algorithm belongs to a blind extraction, enabling it to extract the secret message without referring to the original cover model. Finally, the scheme provides independency for the secret payload embedding and supports progressive message extraction.*

Keywords: 3D steganography, Polygon model, Data embedding, High capacity

1. **Introduction.** Steganography is an important sub-discipline of information hiding [1,2]. It conceals private or secret information within a cover medium. The secret message, also known as the "payload", is first embedded by the sender into the cover medium to produce the stego medium. The embedding is usually aided by secret keys in order to increase the security. Then, the stego medium is delivered to the recipient party through a public channel. Finally, the recipient extracts the secret message by using secret keys. The goal of steganography is to keep the mere presence of the secret message undetectable. Only the sender and the recipient know the secret keys; therefore, third parties are not able to discover the secret message hiding in the stego medium as they are not able to extract the secret message without the legal secret keys. Various types of media can be selected to serve as the cover medium, including text, audio, video, images or three-dimensional (3D) models. Recently, 3D models have been heavily used in various applications including computer animations, computer-generated films and computer