MỘT ĐỀ XUẤT SỬ DỤNG LƯỚI 3D KHÉP KÍN ĐỂ GIẤU TIN

Thái Duy Quý[a*]

[a]*Khoa Công nghệ Thông tin, Trường Đại học Đà Lạt, Lâm Đồng, Việt Nam*

Nhận ngày 04 tháng 01 năm 2016
Chỉnh sửa ngày 03 tháng 03 năm 2016 | Chấp nhận đăng ngày 16 tháng 03 năm 2016

Tóm tắt

Kỹ thuật giấu tin trong đối tượng lưới 3D được đưa ra trong [4], [5] là phương pháp giấu tin trên các đỉnh của một tập các tam giác Theo chuỗi bit khóa sinh ra trong quá trình giấu. Các phương pháp này, trong một số trường hợp, nếu gặp phải lưới hở thì không thực hiện được. Bài báo trình bày phương pháp xác định lưới 3D khép kín, từ đó đề xuất áp dụng các phương pháp giấu tin trong [4], [5] trên kiểu lưới kín đề xuất. Với kỹ thuật này, người nhận chỉ cần biết quy tắc của chuỗi khóa bí mật là có thể giải mã thông tin, sẽ làm tăng tính bảo mật cho các kỹ thuật giấu tin. Thực nghiệm với phương pháp MEP [4] trên các lưới 3D kín cho thấy kỹ thuật này đáp ứng được các yêu cầu giấu tin, có tính bảo mật cao và không cần gửi theo chuỗi bít khóa.

Từ khóa: Giấu tin; Giấu tin mật; Lưới 3D kín; VRML.

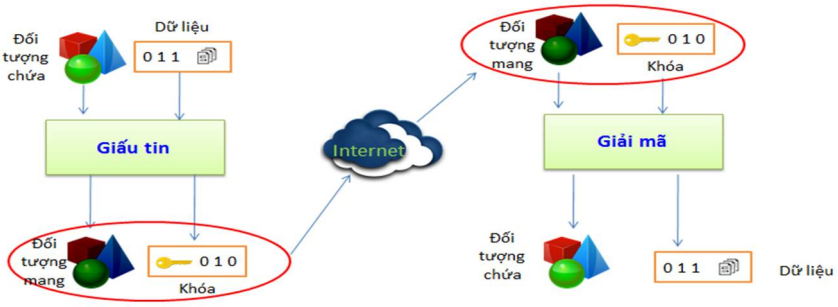
1. GIỚI THIỆU

Giấu tin (data hidding) là kỹ thuật giấu một lượng thông tin dưới dạng một chuỗi bít vào một đối tượng (gọi là đối tượng chứa - *cover*) để trở thành đối tượng khác (đối tượng mang - *stego*). Kỹ thuật này được ứng dụng trong bảo mật dữ liệu và bảo vệ bản quyền tác phẩm. Ưu điểm chính của kỹ thuật này là cả người gửi lẫn người nhận đều khó nhận biết được thông tin đã giấu trong đối tượng [1]. Có nhiều môi trường đa phương tiện được dùng cho giấu tin như ảnh, âm thanh, video, văn bản….

Hình 1 minh họa quá trình giấu tin cơ bản. Quá trình giấu tin được chia thành hai khối có cấu trúc giống nhau: *quá trình nhúng* và *quá trình giải mã*. Quá trình nhúng nhận vào đối tượng chứa, dữ liệu cần nhúng, sau khi thực hiện nhúng thông tin, kết quả sẽ cho ra đối tượng mang và chuỗi bít khóa bí mật, đối tượng mang và khóa bí mật sẽ

* Tác giả liên hệ: Email: quytd@dlu.edu.vn

được chuyển cho người nhận. Quá trình giải mã sử dụng đối tượng mang, quy tắc khóa bí mật để cho ra dữ liệu đã được giấu.



Hình 1. Quá trình nhúng và giải mã thông tin

2. BIỂU DIỄN LƯỚI TAM GIÁC

Trong thập niên gần đây, các kỹ thuật mô hình hóa đối tượng trong không gian ba chiều (3D) được phát triển mạnh và có ứng dụng trong nhiều lĩnh vực đồ họa, mô phỏng, thiết kế.... Có nhiều phương pháp biểu diễn các đối tượng 3D như khối cầu, hình chóp, hình lập phương… Để biểu diễn các đối tượng phức tạp, người ta thường dùng mô hình đối tượng lưới. Trong các loại mô hình lưới, thì lưới tam giác được sử dụng nhiều nhất. Lưới tam giác được xây dựng từ nhiều mặt tam giác, các tam giác này biểu diễn tọa độ các đỉnh và các màu sắc nếu có. Định nghĩa 1 cho thấy một cách biểu diễn lưới tam giác.

Định nghĩa 1. *Cho tập đỉnh $V = [V_1, V_2 \dots V_n]$, với mỗi đỉnh là bộ ba các giá trị tọa độ x, y, z trong không gian, n là tổng số đỉnh. Một biểu diễn lưới tam giác trong không gian ba chiều là một tập cấu trúc lưu trữ thông tin về kết nối giữa các đỉnh:*

$$I = \{I_1; I_2; \dots ; I_k\} \quad (1)$$

Với $1 \le k \le n$. I_i (với $1 \le i \le k$) là bộ 3 các chỉ số (u, v, t) với $1 \le u < v < t \le$ n.

Ví dụ 1: Cho tập $V = [V_1, V_2, V_3, V_4]$.

- Hình chóp C có thể được biểu diễn dưới dạng lưới (Hình 2a):

$$I_C = \{(1,2,3);(1,2,4);(1,3,4);(2,3,4)\}$$

- Hình 2b biểu diễn một lưới tam giác $I_M = \{(1,3,4);(2,3,4)\}$

(a) (b)

Hình 2. Mô hình biểu diễn lưới

Các nghiên cứu trong [3] cho thấy đây cũng là một môi trường giấu tin tốt, đảm bảo lượng thông tin giấu nhiều và vô hình với người gửi lẫn người nhận.

Phương pháp giấu tin mật trong lưới 3D được nghiên cứu bởi các tác giả tại [3, 4, 5]. Trong [4], các tác giả đã đưa ra phương pháp giấu tin mật dựa trên việc biểu diễn một tam giác thành hai trạng thái là 0 và 1, và giấu tin bằng cách dịch chuyển đỉnh. Phương pháp trong [4] có thể giấu được 3 bít trên mỗi tam giác. Các tác giả [5] đã mở rộng phương pháp trong [4] bằng phương pháp nhúng đa cấp (multilevel embedding) trên mỗi tam giác và đã giấu được số lượng bit gần gấp ba lần.

Bài báo này trình bày một đề xuất về kỹ thuật giấu tin mật trên đối tượng lưới tam giác *khép kín* trong lưới tam giác 3D được đưa ra trong [4]. Ý tưởng trong [4] là thực hiện nhúng các bít dựa trên sự dịch chuyển của các tọa độ đỉnh của lưới 3D. Không như kỹ thuật trong [4], đề xuất này coi chuỗi bít khóa dùng để duyệt qua các tam giác là một quy tắc cho trước, khi đó chuỗi bít khóa không cần gửi qua cho người nhận là chuỗi bít dịch chuyển. Kỹ thuật này có thể nhúng được 3 bít trong mỗi tam giác và có thể tiếp tục nhúng bít trên các tam giác đã nhúng trước đó.

3. KỸ THUẬT GIẤU TIN TRONG LƯỚI 3D

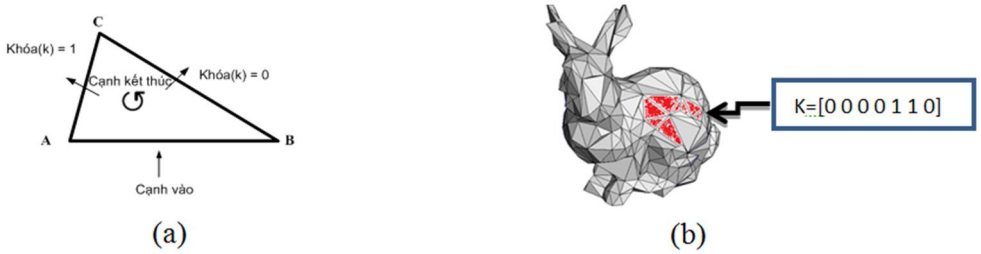
Kỹ thuật giấu tin này được đề xuất trong [4], được gọi là phương pháp MEP, là kỹ thuật giấu tin trên tam giác, thực hiện như trong các phần 3.1 và 3.2.

3.1. Xây dựng danh sách tam giác

Từ một đối tượng lưới tam giác 3D, chọn một tam giác ban đầu và một cạnh ban đầu trong tam giác đó. Trong mỗi một tam giác, định nghĩa một *cạnh vào* là cạnh dùng để đi vào tam giác và hai *cạnh kết thúc* để đi ra tới định tam giác kế tiếp (Hình 3a). Giả

sử từ tam giác ban đầu *ABC* với *AB* là cạnh vào, *AC* và *BC* lần lượt là hai cạnh ra của tam giác, tam giác kế tiếp được tìm ra theo theo quy tắc bit khóa như sau:

- Nếu giá trị bít khóa là "1", tam giác kế tiếp là tam giác kề cạnh BC.
- Ngược lại, nếu giá trị bít là "0" sẽ là tam giác kề cạnh AC.

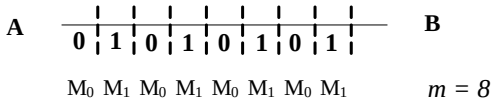


Hình 3. Phương pháp xác định tam giác kế tiếp dựa trên ký tự nhị phân

Như vậy cạnh kết thúc của tam giác này là cạnh vào của tam giác kế tiếp. Hình 3b cho thấy một danh sách các tam giác khi được duyệt tương ứng với chuỗi bit khóa được phát sinh. Độ dài của chuỗi bít khóa bằng độ dài của danh sách các tam giác dùng để lưu các bít. Giả sử cần giấu *M* bít, nếu mỗi đỉnh giấu một bít, số bít khóa sẽ là $n_k = M/3$.

3.2. Giấu tin trong tam giác

Xét tam giác *ABC*, ký hiệu $P(C)|_{AB}$ là hình chiếu của đỉnh *C* lên cạnh *AB*. Khoảng cách *AB* được chia thành hai tập con là M_0 và M_1 biểu diễn các bít luân phiên "0", "1" (M_0 là tập biểu thị cho bít "0", M_1 biểu thị cho bít "1) (Hình 4).

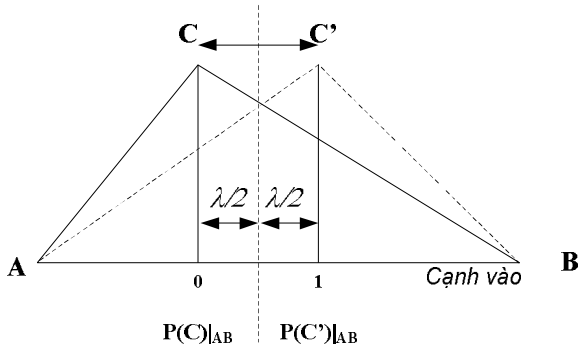


Hình 4. Minh họa chia |AB| thành hai tập M_0 và M_1 với m = 8

Để nhúng bít thứ *i* (*i = 0 hoặc 1*) vào đỉnh *C*, xét hai trường hợp:

- Nếu $P(C)|_{AB} = M_i$: Không cần thực hiện sự thay đổi nào cả.
- Nếu $P(C)|_{AB} \neq M_i$: Đỉnh *C* dịch chuyển qua *C'* sao cho $P(C')|_{AB} = M_i$.

Quá trình được minh họa trong Hình 5.



Hình 5. Quá trình dịch chuyển đỉnh C thành C'.

Đỉnh C' có thể được lấy đối xứng với đỉnh C qua trục đối xứng là biên của miền giá trị M_0 và M_1 nằm ở gần nhất. Giá trị λ được gọi là *khoảng phân đoạn*, và được tính bằng: $\lambda = |AB|/m$ với m là tổng số tập con M_i ($i = 0$ *hoặc* 1). Tọa độ vị trí mới C' được tính bằng (1).

$$x_{C'} = x_C + a\frac{\lambda}{\sqrt{a^2+b^2+c^2}},\ y_{C'} = y_C + b\frac{\lambda}{\sqrt{a^2+b^2+c^2}},\ z_{C'} = z_C + c\frac{\lambda}{\sqrt{a^2+b^2+c^2}} \quad (2)$$

Trong đó a, b, c là tọa độ của vector chỉ phương AB, λ là giá trị khoảng phân đoạn. Giá trị λ phải đủ lớn để làm thay đổi trạng thái của tam giác từ *"0"* qua *"1"* hoặc từ "1" qua "0" và cũng phải đủ nhỏ để sau khi dịch chuyển không làm biến đổi nhiều hình dạng ban đầu.

3.3. Kỹ thuật giải mã thông tin

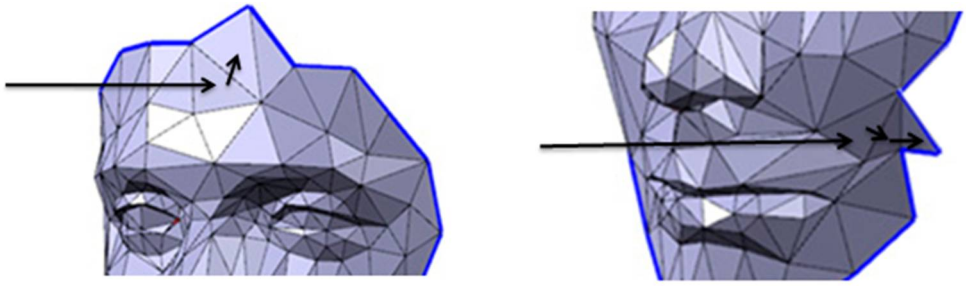
Kỹ thuật giải mã thông tin cũng thực hiện duyệt danh sách các tam giác giấu tin khi biết chuỗi bit khóa bí mật. Tuy nhiên trong bước giải mã sẽ thực hiện các thao tác ngược lại so với kỹ thuật giấu tin.

3.4 Nhận xét

Phương pháp trong [4] (thậm chí trong [5]) gặp phải các vấn đề như sau:

Vấn đề 01: Khi duyệt qua các đỉnh dựa trên chuỗi khóa, nếu gặp trường hợp tới một tam giác chỉ có một tam giác kề trong khi đó bit khóa không thuộc tam giác đó

(Hình 6a) hoặc không có tam giác kề nào (Hình 6b) thì không thể phát sinh bit khóa tiếp theo, lúc này chương trình sẽ bị ngưng và không giấu được thông tin.



(a) (b)

Hình 6. Minh họa quá trình duyệt tam giác phát sinh bit khóa

Vấn đề 02: Việc chuyển thông tin cho người nhận, ngoài đối tượng mang, còn phải kèm theo chuỗi bit khóa, điều này gây khó khăn trong quá trình bảo mật.

3.5 Hướng đề xuất

Sử dụng lưới tam giác khép kín để giấu thông tin, với *vấn đề 01* lưới tam giác kín sẽ luôn có ba tam giác kề tam giác cho trước, việc duyệt các tam giác giấu tin sẽ diễn ra thuận tiện mà không bị ngưng. Trong *vấn đề 02*, có thể sử dụng một quy tắc khóa bí mật cho trước, thống nhất giữa chương trình giấu tin và giải mã, khóa sẽ được phát sinh theo quy tắc đó.

Vấn đề đặt ra ở đây là làm thế nào xác định được lưới nào kín, lưới nào không kín để giấu thông tin, mục tiếp theo sẽ đưa ra hướng giải quyết dựa trên một định nghĩa về lưới kín và một định lý dùng để xác định lưới kín.

4. LƯỚI 3D KHÉP KÍN

Lưới 3D khép kín thực chất là mô hình lưới 3D không có lỗ thủng trên bề mặt. Về mặt biểu diễn thì một lưới kín phải biểu diễn thông số của tất cả các đỉnh.

Định nghĩa 2. *Cho tập đỉnh V, một lưới tam giác 3D khép kín là một tập cấu trúc lưu trữ thông tin kết nối giữa các đỉnh sao cho với mọi tam giác ta luôn tìm được 3 tam giác kề tương ứng với 3 cạnh của tam giác đó.*

Ví dụ 2: Trong Ví dụ 1 hình chóp I_C = *{(1,2,3);(1,2,4);(1,3,4);(2,3,4)}* là một lưới khép kín vì dựa vào cấu trúc lưu trữ cho thấy bất kỳ tam giác nào cũng luôn có 3 tam giác kề với 3 cạnh.

Định lý*: Cho tập V và bộ biểu diễn lưới I. Với mọi cặp* $(u,v) \in I_i$ *với* $1 \le i \le k$ *(k là số mặt tam giác của lưới), nếu luôn tìm được số tự nhiên* $t \ne u,v$ *sao cho bộ* $(u,v,t) \in I\{I_i\}$ *thì cấu trúc lưu trữ lưới là khép kín.*

Chứng minh:

Nếu có cặp (u,v) nhưng không tìm được t để tạo thành bộ $(u,v,t) \in I$, lúc này u,v là 2 chỉ số đỉnh tương ứng của V_u, V_v. Như vậy không tồn tại đỉnh V_t để tạo thành tam giác $V_uV_vV_t$. Như vậy cạnh V_uV_v không có tam giác liền kề với nó, theo định nghĩa 2.2 lưới *(V,I)* không là lưới khép kín.

Từ định lý trên, ta có thuật toán kiểm tra lưới kín như sau.

Input: Lưới tam giác (V,I)

Output: Lưới kín hay không.

Thuật toán 1:

Bước 1: khởi tạo $i = 1$;

Bước 2: Với $\forall I_i$, lấy bộ $(u,v) \in I_i$. Nếu $\exists t\ (1 \le t \le n;\ t \ne u,\ t \ne v)$ sao cho $(u,v,t) = I_j\ \forall i \ne j$ thì lưới là khép kín. Ngược lại: Lưới không khép kín.

Ứng dụng: Các lưới 3D khép kín biểu diễn các tam giác liền nhau, và vì vậy khi duyệt các tam giác để xác định các tam giác giấu tin ta có thể duyệt liên tục mà không bị ngừng lại.

5. GIẤU TIN TRÊN LƯỚI 3D KHÉP KÍN

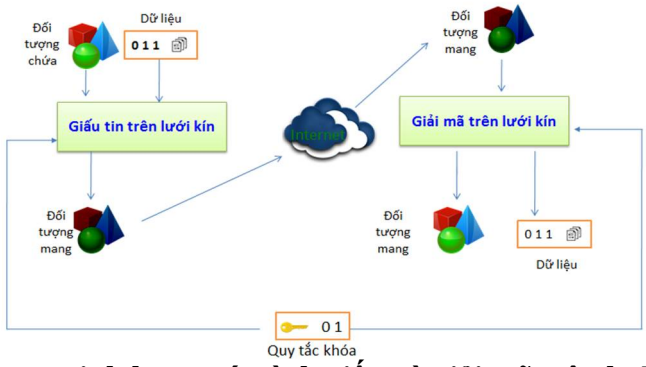
Dựa trên các định nghĩa và định lý ở mục 4, có thể áp dụng phương pháp giấu tin trên lưới 3D khép kín với các bước như sau:

Bước 1: Kiểm tra lưới kín hay hở bằng Thuật toán 1

Bước 2: Nếu lưới kín thì giấu tin theo phương pháp [4] đã trình bày ở mục 3.

Bước giải mã thông tin: có thể thực hiện ngược lại các bước như giấu tin với quy tắc khóa cho trước.

Mô hình giấu tin và giải mã thông tin có thể thực hiện như trong Hình 7. Lúc này chuỗi bit khóa bí mật được thống nhất trong chương trình gửi và nhận. Kỹ thuật này đòi hỏi thêm một bước kiểm tra lưới 3D kín hay hở, nếu kín thì thực hiện giấu tin, nếu lưới hở có thể bỏ qua.

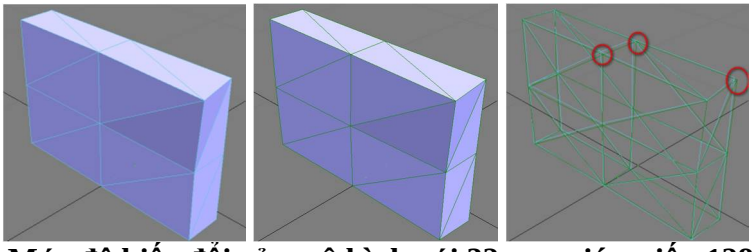


Hình 7. Minh họa quá trình giấu và giải mã trên lưới kín

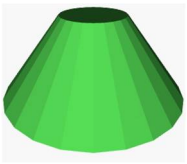
6. KẾT QUẢ THỰC NGHIỆM

Chương trình thực nghiệm thực hiện trên các mô hình VRML, sử dụng giá trị *m = 100*. Quy tắc của chuỗi bít khóa được sử dụng là chuỗi bít luân phiên 0 và 1.

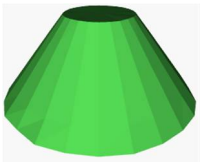
Hình 8 và Hình 9 cho thấy sự có sự biến đổi với trường hợp giấu nhiều bít trên một số lượng tam giác ít. Kết quả rút trích giống ban đầu nhưng mô hình đã có sự biến đổi, về mặt tổng thể, mô hình vẫn giữ được nguyên bản ban đầu.



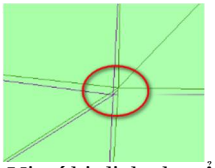
Hình 8. Mức độ biến đổi của mô hình với 32 tam giác, giấu 128 bít tin.



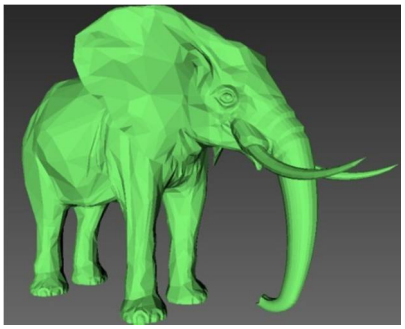
(a) Mô hình nhúng cone.vrl



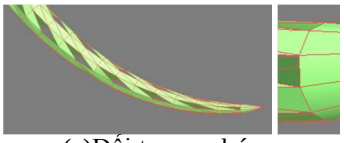
(b) Đối tượng mang s_cone.vrl



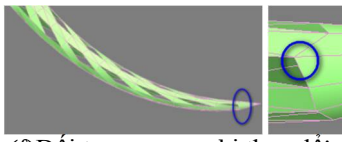
(c) Vị trí bị dịch chuyển.



(d) Mô hình Elephant



(e)Đối tượng nhúng



(f)Đối tượng mang bị thay đổi

Hình 9. Thử nghiệm nhúng trên một số mô hình.

Kết quả thực nghiệm cho thấy tỉ lệ rút trích đạt kết quả tốt, tuy nhiên việc giấu quá nhiều thông tin trên một mô hình sẽ làm mô hình bị biến đổi nhiều. Chính vì vậy mà kỹ thuật này đạt kết quả tốt nhất với lượng bít giấu bằng số tam giác. Nếu mỗi tam giác chỉ giấu ba bít, công thức tính số bít giấu hiệu quả là $n_{bit} = 3k$ với k là số tam giác giấu.

7. KẾT LUẬN

Bài báo đề xuất phương pháp xác định lưới 3D khép kín, từ đó áp dụng phương pháp giấu tin dựa trên cấu trúc lưới này. Kỹ thuật giấu tin trong môi trường lưới tam giác khép kín vẫn đảm bảo được các tính chất giống như giấu tin trên các môi trường khác. Kết quả của bài báo có thể ứng dụng trong lĩnh vực bảo vệ bản quyền, chuyển tin mật, xác lập thông tin…

TÀI LIỆU THAM KHẢO

[1] W.Bender, D.Gruhl, N.Morimoto and A.Lu, *Techniques for data hidding*, IBM Systems Journal, Vol 35, Nos 3&4, (1996).

[2] Min Wu, *Multimedia Data Hiding*, Princeton University, USA,(2001).

[3] Jingliang Peng, Chang-Su Kim and C.-C. Jay Kuo, *Technologies for 3D mesh compression: A survey*, Journal of Visual Communication and Image Representation, Volume 16, Issue 6, December 2005, Pages 688-733, (2005).

[4] François Cayre and Benoît Macq, Data Hiding on 3-D Triangle Meshes, IEEE Transaction on signal processing, (2003).

[5] Yu-Ming Cheng, Chung-Ming Wang, A high-capacity steganographic approach for 3D polygonalmeshes, Visual Comput, (2006).

[6] Min-Wen Chao, Chao-hung Lin, Cheng-Wei Yu, and Tong-Yee Lee, A *High Capacity 3D Steganography Algorithm*, IEEE Transactions on Visualizations and Computer Graphics, (2009).

STEGANOGRAPHY TECHNIQUE ON CLOSED 3D TRIANGULAR MESHES

Thai Duy Quy[a*]

[a]*The Faculty of Information Technology, Dalat University, Lamdong, Vietnam*
[*]*Corresponding author: quytd@dlu.edu.vn*

Article history
Received: January 04th, 2016
Received in revised form: March 03rd, 2016
Accepted: March 16th, 2016

Abstract

This paper proposes a structure presentation of 3D mesh and closed mesh, which can apply for hidden messages. Based on shifting value coordinates of vertices, the technique allows information hidden on the triangular 3D mesh model. This above process is controled by rule secret key. The article also mentions a reverse to decode data from stego.

Keywords: 3D Modelling; Data hiding; Steganography; VRML.