Annual of Konstantin Preslavsky University of Shumen
vol. XXIII C, 2022, pp. 23 – 28, https://doi.org/10.46687/EBZG7189

MODIFICATION OF 3D MODELS FOR THE PURPOSES OF STEGANOGRAPHY [*]

DELYAN H. SARMOV

ABSTRACT: *Steganography uses three-dimensional file formats as a carrier of information. There are different algorithms in which the existing information about the model is changed or new information is added without visually changing the model. This paper proposes a method by adding vertices involved in the triangular mesh of the model.*

KEYWORDS: *3D models; vector graphic; obj; steganography; Stego methods; Information hiding; Information security*

2020 Math. Subject Classification: *68P20, 68P25*

МОДИФИЦИРАНЕ НА 3D МОДЕЛИ ЗА ЦЕЛИТЕ НА СТЕГАНОГРАФИЯТА[†]

ДЕЛЯН Х. СЪРМОВ

1 Въведение

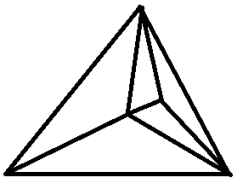
Съществуват различни подходи за скриване на информацията в текст изображения или мултимедийни файлове. Необходимостта от създаване на защитени канали за предаване на информация, изисква разработване на стенографски методи с използване на различни контейнери. В тази статия се разглежда метод за скриване на информация във файлове с векторна

[*]This paper is (partially) supported by Scientific Research Grant РД-08-147/02.03.2022

[†]Статията е частично финансирана по проект № РД-08-47/02.03.2022

триизмерна графика, като за целта се добавя информация за нови точки в геометричния модел (вертекси).

Използваните до момента сходни алгоритми използват разделяне на добавяне на нов вертекс във вътрешността на триъгълника, при което се получават 3 резултантни триъгълника (Фиг. 1.). В координатите на добавената точка се скрива част от съобщението. Процесът се повтаря рекурсивно до изчерпване на съобщението.[1,2,3]

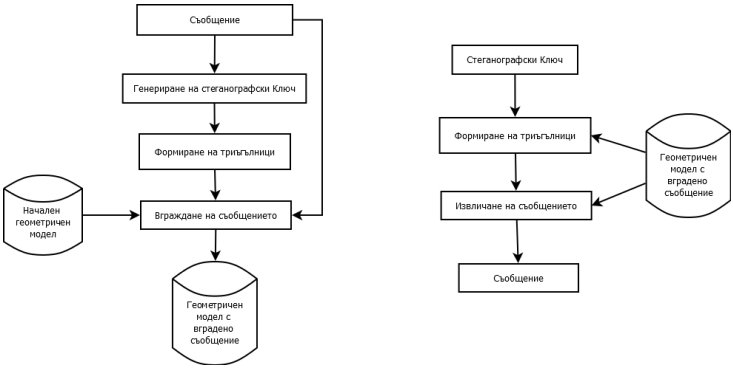


Фиг. 1. Формиране на нови триъгълници с добавяне на вертекс във вътрешността на триъгълника

2 Изложение

В настоящата статия се предлага разделяне с нови вертекси на страните на триъгълниците рекурсивно. Така се получават 4 нови триъгълника, които се използват като носител на скритата информация. Не се засягат първоначално съществуващите вертекси, поради което процеса е обратим и не се губи оригиналната информация. Използва се симетричен стеганографски ключ, който се генерира динамично в зависимост от съобщението и контейнера.

Процесът може да се раздели на 4 етапа: генериране на ключ, добавяне на вертекси, вмъкване на съобщението и извличане на съобщението (Фиг. 2.).



Фиг. 2. Процес на вмъкване и извличане на съобщението

Генериране на ключ

- Всеки символ от съобщението се конвертира по избрана ASCII таблица в число и в последствие се представя в двоична форма. Така представеното съобщение обозначаваме с M.

- M се разделя на блокове от по 3 бита, където d_1, d_2, …. d_k са числата в 3 битовите блокове.

- d_i, където 1<i<k се нормализира по формулата: $d_i = \frac{d_i - min}{max - min}$ където min е минималното d_i , max е максималното d_i

- Изчислява се d_{mid} като средно аритметично на вече нормализираните d_i

- d_{mid} се използва за получаване на стеногрфския ключ K=d_{mid}*N, където N е числова стойност зависеща от файла контейнер. Може да се използва големината на файла, името му, дата и час на създаване или друга негова характеристика.

По този начин стеногрфският ключ се генерира в зависимост от файла контейнер и съобщението. Малка промяна в съобщението дава напълно различен ключ. В следващата стъпка

d_{mid} участва във формирането на нови триъгълници, както и при извличане на съобщението.

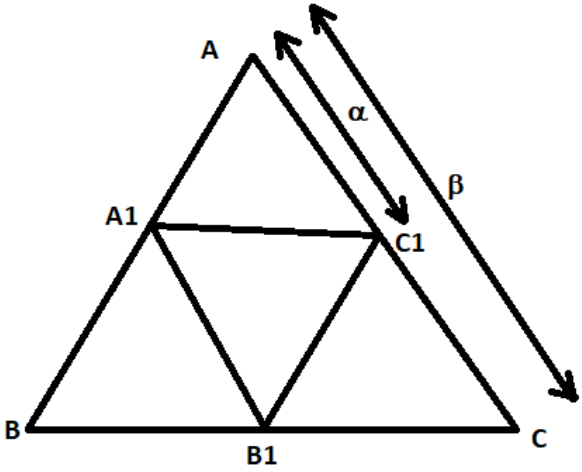
Формиране на нови вертекси

Необходими са 3 върха за да се получи нов триъгълник във вътрешността на съществуващ.

- нека i=0 . Дължината на текущо обработваната страна е β, а разстоянието между първия връх на страната и новия вертекс е α. (Фиг. 3.)

$\alpha=\beta*d_{mid}$, където $d_{mid}=K/N$ се получава от стеганографския ключ.

За определеност страните се обхождат по часовниковата стрелка, докато се получи нов триъгълник.



Фиг. 3. Формиране на нови триъгълници

- Предходната стъпка се повтаря рекурсивно за триъгълника $A_1B_1C_1$ или за четирите нови триъгълника $A_1B_1C_1$, AC_1A_1, C_1CB_1 и A_1B_1B, докато

$i < \frac{l}{3 * n}$, където „l“ дължината на съобщението, а „n“ е броя на битовете записвани във вертекс. „n“ се избира от потребителя.

Обозначаваме новополучените вертекси с V_{ij} (1<=i<=t, 1<=j<=3), където t е броя на триъгълниците.

Вмъкване на съобщението

- Изчисляване на координатите на вертексите V_{ij} (1<=i<=t, 1<=j<=3)
- Преобразуване на стеганографския ключ в двоичната му форма
- вмъкване на съобщението в информацията за вертексите с промяна на най-малко значещия бит (LSB). [4,5]

Извличане на съобщението

- Стеганографският ключ се изпраща до получателя по сигурен канал.
- От стеганографския ключ се получава d_{mid}=K/N
- Извличат се вертексите, в които е съхранено съобщението с използване на d_{mid} . Използваните вертекси са извлечени, когато не бъде открит вертекс на разстояние d_{mid} от първия връх на текущо обработваната страна.
- Извлича се съобщението.

3 Заключение

Посоченият метод добавя нови вертекси във векторни файлови формати, с което може да се адаптира капацитета на носителя (файла) към големината на съобщението. Визуално геометричния модел се съхранява при използване на LSB.

Възможни са различни вариации на алгоритъма с използване на един или четири резултатни триъгълника. Допълнителни изследвания изисква използване на итеративен алгоритъм с вграждане на точно един триъгълник (три вертекса) в

първоначално съществуващите триъгълници в модела. Както и използване на полигони с повече от три върха.

Стеганографският ключ се генерира на базата на съобщението и файла контейнер. Ако вместо с LSB за модификация на информацията за вертексите се променят значими битове, методът е подходящ за употреба в областта на защита на авторските права.[6]

ЛИТЕРАТУРА:

[1] Ashish Girdhar, Vijay Kumar, A reversible and affine invariant 3D data hiding technique based on difference shifting and logistic map, Journal of Ambient Intelligence and Humanized Computing, 10.1007/s12652-019-01179-4, 10, 12, (4947-4961), (2019).

[2] Sara Farrag, Wassim Alexan, Secure 3D data hiding technique based on a mesh traversal algorithm, Multimedia Tools and Applications, 10.1007/s11042-020-09437-w, 79, 39-40, (29289-29303), (2020).

[3] Girdhar, Ashish & Chahar, Vijay. (2017). Comprehensive Survey of 3D Image Steganography Techniques. IET Image Processing. 12. 10.1049/iet-ipr.2017.0162.

[4] Kordov, K., Stoyanov, B. (2017). Least Significant Bit Steganography using Hitzl-Zele Chaotic Map. International Journal of Electronics and Telecommunications, Vol. 63, No. 4, pp. 417-422

[5] Gaur, Shubh & Chaturvedi, Swati & Gupta, Shiavnsh & Mittal, Jay & Tanwar, Rohit & Goswami, Mrinal. (2023). Image Distortion Analysis in Stego Images Using LSB. 10.1007/978-981-19-1142-2_52.

[6] El Hanafy, Yara. (2022). Watermarking 3D Models. 10.13140/RG.2.2.30172.46724.

Делян Христов Сърмов
ШУ „Епископ Константин Преславски“
E-mail: d.sarmov@shu.bg