EXPLORING STEGANOGRAPHIC PROTECTION POSSIBILITIES IN 3D OBJECTS

STOYAN V. STOYANOV

ABSTRACT: *This paper examines the structure of 3D objects to determine the potential possibilities for steganographic information protection. Identifying the appropriate structural elements is of paramount importance for developing a secure steganographic algorithm for data hiding.*

KEYWORDS: *Steganography, 3D steganography, Data hiding.*

DOI: https://doi.org/10.46687/GFGX7021

ИЗСЛЕДВАНЕ НА ВЪЗМОЖНОСТИ ЗА СТЕГАНОГРАФСКА ЗАЩИТА В 3D ОБЕКТИ [*]

СТОЯН В. СТОЯНОВ

АБСТРАКТ: *Настоящата статия разглежда структурата на 3D обекти за определяне на потенциалните възможности за стеганографска защита на информация. Определянето на подходящите структурни елементи е от първостепенно значение за разработването на сигурен стеганографски алгоритъм при скриването на данни.*

1 Въведение

Развитието на информационните и комуникационните технологии води до непрекъснато увеличаване на количеството цифрова информация, която се създава, обработва и предава. Наред с традиционните текстови документи[1], изображения[2,3], аудио[4] и видеофайлове[5], все по-широко приложение намират цифровите триизмерни обекти[6]. Те се използват в компютърната графика, медицината, архитектурата, инженерното проектиране, виртуалната и разширената реалност, компютърните игри и адитивното производство.

Широкото разпространение на 3D съдържание създава необходимост от разработването на методи за защита, удостоверяване на произхода и скриване на информация в триизмерни обекти. Един от възможните подходи е използването на стеганография. За разлика от криптографията, при която съдържанието на съобщението се преобразува в неразбираема форма, стеганографията цели да прикрие самото наличие на тайна информация. Съобщението се вгражда в цифров носител по начин, който не трябва да предизвиква основателни подозрения за извършената промяна.

Като носители на скрита информация традиционно се използват цифрови изображения, аудиосигнали, видеозаписи и текстови документи. Триизмерните обекти предлагат допълнителни възможности, тъй като могат да съдържат голям брой геометрични, топологични и визуални компоненти. При полигоналните мрежи това са координатите на върховете, ръбовете, лицата, нормалните вектори, цветовете и

[*] Настоящата статия е частично финансирана по проект № РД-08-88/02.02.2026.

текстурните координати. Тези елементи могат да бъдат използвани самостоятелно или в комбинация като области за вграждане на информация.

Публикуваните изследвания класифицират методите за стеганография в 3D мрежи основно като методи в двусъстояниева, LSB, пермутационна и трансформационна област. В практическите разработки най-често се използват координатите или последователността на върховете, тъй като те предоставят сравнително голямо пространство за вграждане [7].

Използването на 3D обекти за стеганографски цели обаче създава редица проблеми. Вградената информация може да бъде повредена при мащабиране, ротация, изглаждане, опростяване на полигоналната мрежа, повторна триангулация или преобразуване между файлови формати. Освен това изменението на геометрията може да бъде открито чрез статистически анализ на координатите и локалните характеристики на повърхността.

Целта на настоящата статия е да бъдат изследвани структурните компоненти на цифровите 3D обекти и да бъдат определени техните потенциални възможности за стеганографско скриване на информация. За постигане на целта се разглеждат основната структура на цифровите 3D обекти, възможните области за вграждане, критериите за оценяване, основните въздействия върху скритата информация и изискванията към бъдещ стеганографски алгоритъм.

2 Структура на цифровите 3D обекти

Триизмерният цифров обект може да бъде представен по различни начини. Сред основните представяния са облаците от точки, вокселните модели и полигоналните мрежи. Облакът от точки представлява множество от самостоятелни точки в триизмерното пространство. Вокселният модел разделя пространството на регулярна триизмерна решетка от обемни елементи. Полигоналната мрежа описва повърхността на обекта чрез върхове, ръбове и лица.

Полигоналните мрежи са предпочитан носител при значителна част от изследванията върху 3D стеганографията, тъй като предоставят голям брой възможни области за вграждане. Освен геометричните координати те могат да съдържат топологични зависимости и допълнителни атрибути [7, 8].

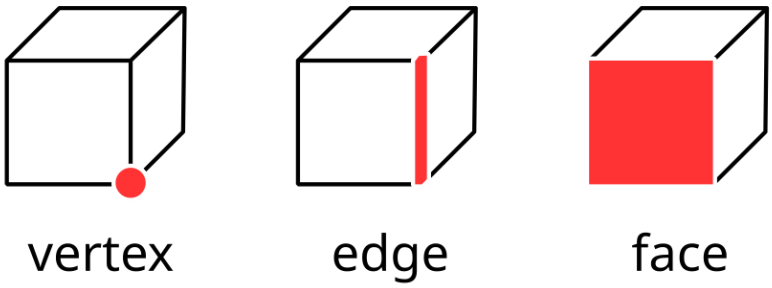
Една полигонална мрежа може да бъде представена чрез M = (V, E, F, A), където V е множеството от върхове, E е множеството от ръбове, F е множеството от лица, а A е множеството от допълнителни атрибути.

2.1. Върхове, ръбове и лица

Върховете определят основните геометрични позиции, чрез които се изгражда повърхността. Всеки връх може да бъде представен като $v_i = (x_i, y_i, z_i)$, където x_i, y_i и z_i са координатите по трите пространствени оси. При n върха моделът съдържа 3n координатни стойности, което създава значителен теоретичен капацитет за вграждане.

Ръбът представлява връзка между два върха и определя част от топологичната структура на модела. Ръбовете позволяват да се установят съседните върхове и да се изследват локални характеристики като дължина, ъгъл между лица и изменение на повърхността.

Лицата определят отделните повърхностни елементи. Най-често се използват триъгълни лица, тъй като улесняват обработката и визуализацията. При определени условия една и съща или приблизително еднаква повърхност може да бъде представена чрез различно разположение на вътрешните ръбове. Това създава възможност топологията да участва в кодирането на информация. На ***Фигура 1*** са показани основните структурни елементи на полигоналната мрежа на 3D обект.



Фигура 1 - Основни структурни елементи на полигонална мрежа: връх, ръб и лице (Източник: Wikimedia Commons)

2.2. Нормални вектори и визуални атрибути

Нормалният вектор определя ориентацията на дадено лице или връх спрямо повърхността. За триъгълно лице ненормираният нормален вектор се определя чрез векторно произведение на два от неговите ръбове, а след нормализиране дължината му е единица. Нормалите участват при осветяването и изглаждането и могат да бъдат съхранявани във файла или преизчислявани от геометрията.

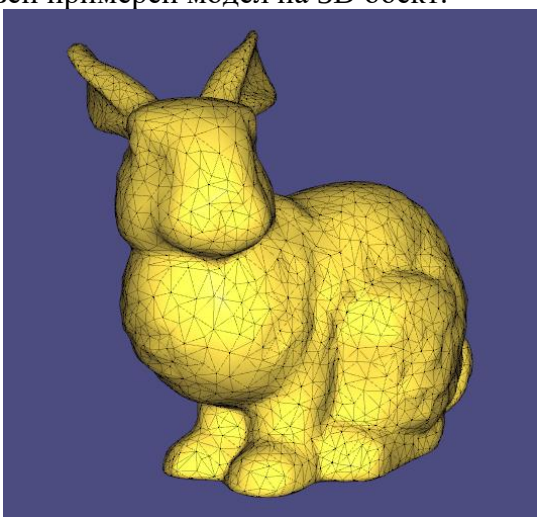
Освен геометрична информация, 3D моделът може да съдържа цвят за всеки връх, прозрачност, текстурни координати, изображения за текстури, материали и коефициенти за отражение. Тези атрибути разширяват възможностите за вграждане, но използването им зависи от файловия формат и от начина на импорт и експорт.

2.3. Влияние на файловия формат

Структурата, която се запазва във файла, зависи от използвания формат. OBJ може да съдържа позиции на върхове, нормални вектори, текстурни координати и лица. STL представя предимно триъгълна геометрия и нормали на триъгълниците. PLY може да съдържа върхове и лица, както и допълнителни характеристики за всеки връх, например цвят, нормала или потребителски дефинирана стойност.

Тази разлика е съществена за стеганографията. Ако съобщението е вградено в структурен компонент, който не се поддържа от целевия формат, информацията ще бъде загубена при конвертиране. Следователно файловият формат трябва да се разглежда като част от стеганографската система, а не единствено като контейнер за геометрията.

На ***Фигура 2*** е представен примерен модел на 3D обект.



Фигура 2 - Полигонално представяне на тестовия модел Stanford Bunny (Източник: G1malitm, Mesh bunny.png, Wikimedia Commons)

3 Структурни елементи, подходящи за скриване на информация

3.1. Координати на върховете

Координатите са една от най-перспективните области за вграждане. Основната идея е отделни стойности да бъдат изменени с достатъчно малка величина, така че разликата между оригиналния и получения обект да не бъде визуално забележима.

Нека $m_i \in \{0,1\}$ е бит от тайното съобщение. Координатата x_i може първо да се преобразува в целочислена стойност $q_i = \text{round}(x_i \times 10p)$. След това младшият бит се заменя с m_i, а модифицираната координата се възстановява чрез $x'i = q'i / 10p$. Стойността p определя точността. При по-голяма стойност изменението е по-малко, но вероятността информацията да бъде унищожена при закръгляване или конвертиране се увеличава.

Изследвани са и подходи, при които се променят четвъртият и петият знак след десетичната точка на координатите. Те могат да осигурят добро визуално сходство, но зависят от точността, която се запазва при последваща обработка [10]. Предимствата са голям брой стойности за вграждане, сравнително проста реализация, псевдослучаен избор на върхове и възможност за адаптиране спрямо локалната геометрия. Недостатъците включват чувствителност към квантуване, изглаждане и геометрични преобразувания, както и риск от статистическо откриване. Примерен обобщен стеганографски модел е представен на ***Фигура 3***.



Фигура 3 - Обобщен модел на процесите по вграждане и извличане на информация в 3D обект.

3.2. Последователност на върховете и лицата

В много случаи промяната на реда на върховете не изменя визуалната форма, ако индексите във всички лица бъдат актуализирани правилно. Информация може да бъде кодирана чрез взаимното разположение на два или повече върха. Предимството е, че координатите не се променят и не се въвежда геометрично изкривяване. Подобен подход може да се приложи и към реда на лицата. Последователността на триъгълниците обикновено не влияе върху геометрията, поради което може да представя двоична информация. Пермутационните методи са самостоятелен клас в съвременните класификации [7]. Слабостта е ниската устойчивост. Софтуерът за обработка може автоматично да сортира елементите, да премахне дублиращи се върхове, да създаде нови индекси или да промени реда при записване. Визуалната форма остава непроменена, но съобщението се унищожава.

3.3. Топологична свързаност

Топологията определя начина, по който върховете, ръбовете и лицата са свързани. При четири приблизително копланарни върха могат да се използват два различни диагонала. Едната конфигурация може да представя бит 0, а другата бит 1, без значително изменение на формата. Недостатък е чувствителността към повторна триангулация, опростяване на мрежата, добавяне или премахване на ръбове и коригиране на топологични дефекти. Топологичните промени могат да създадат и неестествени конфигурации, които влияят върху визуализацията или се откриват при анализ.

3.4. Нормални вектори, цветове и текстури

Компонентите на нормалните вектори могат да бъдат изменяни с малки стойности. Това предлага добър капацитет, но нормалите често се преизчисляват автоматично въз основа на геометрията. След преизчисляването скритите стойности се губят. Освен това компонентите не са напълно независими, защото нормалният вектор трябва да запази единична дължина. При модели с цветове на върховете информация може да бъде вградена в младшите битове на червения, зеления и синия компонент. Подходът е сходен с LSB стеганографията при изображения. Малките изменения обикновено трудно се забелязват, но не всички формати поддържат цвят за всеки връх. Текстурните координати определят съответствието между 3D повърхността и пикселите от текстурното изображение. Минимални промени в координатите или директно в текстурата могат да носят данни. При смяна на текстурата, преоразмеряване на изображението, ново UV разгъване или премахване на материалите съобщението може да бъде загубено.

3.5. Метаданни и допълнителни полета

Някои формати позволяват съхраняване на коментари, имена, потребителски свойства и незадължителни полета. Те дават лесен начин за добавяне на данни, без да се променя видът на обекта. Този подход обаче не осигурява достатъчна стеганографска сигурност. Полетата могат да бъдат открити чрез обикновен преглед на файла и лесно отстранени чрез изчистване или конвертиране. Затова метаданните са по-подходящи за маркиране, отколкото за сигурна тайна комуникация.

4 Критерии за оценяване

Изборът на подходящ структурен елемент трябва да се извършва според общ набор от критерии. Не е достатъчно даден компонент просто да позволява промяна. Трябва да бъде оценено как тя влияе върху сигурността, качеството и използваемостта на 3D обекта.

4.1. Капацитет и незабележимост

Капацитетът характеризира количеството информация, което може да бъде скрито. Ако в n_s структурни елемента се вграждат по b бита, теоретичният капацитет е C = ns x b. Реалният капацитет е по-нисък, защото част от данните се използват за дължина, контролна сума, корекция на грешки и синхронизация. Незабележимостта показва дали промените могат да бъдат възприети визуално или установени чрез геометрично сравнение. Тя може да се оценява чрез средно и максимално преместване на върховете, разстояние между повърхностите, изменение на нормалите и локалната кривина, както и чрез визуално сравнение при различно осветяване.

4.2. Устойчивост и надеждност

Устойчивостта показва дали съобщението може да се извлече след обработка на обекта. За оценяването ѝ могат да се приложат транслация, ротация, мащабиране, изглаждане, квантуване, опростяване, конвертиране и добавяне на геометричен шум. Надеждността може да бъде измерена чрез коефициента на битовите грешки BER = Ne / Nt, където Ne е броят на неправилно извлечените битове, а Nt е общият брой вградени битове. Стойност BER = 0 означава извличане без грешки.

4.3. Сигурност срещу стегоанализ

Стегоанализът цели да определи дали обектът съдържа скрита информация. При 3D мрежите могат да бъдат изследвани разпределенията на координатите, дължините на ръбовете, двустенните ъгли, локалните нормали, кривината и закономерностите в младшите битове. Съвременните адаптивни подходи се стремят да запазят както визуалните, така и стегоаналитичните характеристики на мрежата. Измененията се разпределят така, че да се минимизира предварително дефинирана функция на изкривяването [8, 9].

5 Сравнително изследване на структурните елементи

Резултатите от качествения сравнителен анализ са представени в Таблица 1. Оценките са относителни и се отнасят до общите свойства на структурните елементи. Конкретните резултати зависят от използвания алгоритъм, вида на модела, размера на съобщението и приложените операции.

Таблица 1 - Сравнителна оценка на структурните елементи

Структурен елемент	Капацитет	Незабележимост	Устойчивост	Риск	Приложимост
Координати на върховете	Висок	Висока	Средна	Среден	Много висока
Ред на върховете	Среден	Много висока	Ниска	Нисък-среден	Средна
Ред на лицата	Среден	Много висока	Ниска	Нисък	Средна
Топологична свързаност	Среден	Висока	Ниска	Среден	Средна
Нормални вектори	Висок	Висока	Ниска	Среден	Средна
Цветове на върховете	Висок	Висока	Ниска-средна	Среден	Висока
Текстурни координати	Среден	Висока	Ниска	Среден	Средна
Метаданни	Висок	Не влияе	Много ниска	Много висок	Ниска

Обобщение на сравнението:

Координатите на върховете предоставят най-добър общ баланс. Те присъстват във всички полигонални модели и броят им нараства заедно с геометричната сложност. Използването им позволява разработването на алгоритъм, който адаптивно избира подходящи области и ограничава преместването. Последователността на върховете и лицата предлага отлична визуална незабележимост, тъй като геометрията не се променя. Ниската устойчивост при импорт, експорт и оптимизация ограничава практическото приложение. Нормалните вектори и цветовете могат да осигурят допълнителен капацитет, но не са еднакво поддържани от всички формати и могат да бъдат преизчислени или премахнати. Метаданните позволяват лесно добавяне на информация, но не осигуряват необходимото ниво на сигурност. На тази основа координатите на адаптивно подбрани върхове могат да бъдат определени като най-подходяща основна област за бъдещ стеганографски алгоритъм. Цветове или нормали могат да се използват като помощни области, когато форматът и приложението позволяват това.

6 Основни проблеми при стеганографската защита

6.1. Геометрични преобразувания и квантуване

Транслацията добавя един и същ вектор към координатите, мащабирането ги умножава по коефициент, а ротацията ги преобразува чрез ротационна матрица. Ако информацията е вградена директно в абсолютните координати, тези операции могат да попречат на извличането. Възможно решение е нормализиране на модела преди вграждане и извличане или използване на относителни геометрични характеристики.

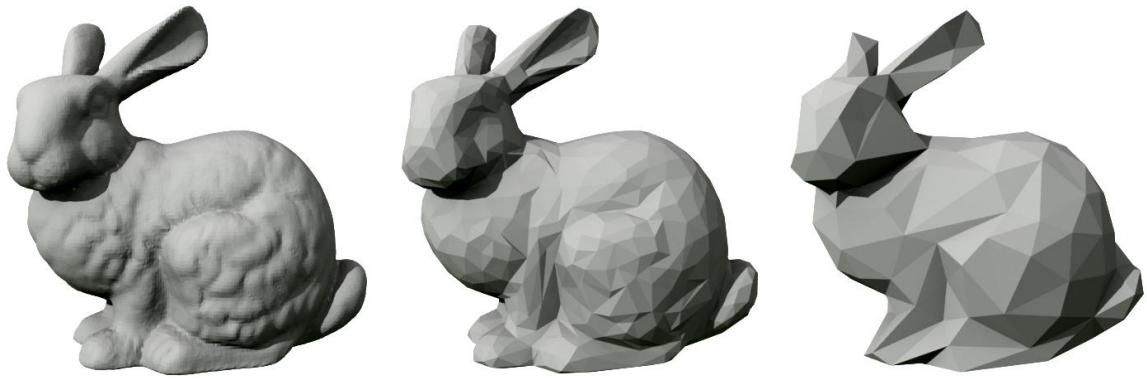
При записване координатите могат да бъдат закръглени до определен брой знаци. Ако съобщението е разположено в по-ниските разреди, то ще бъде унищожено. Следователно точността на файловия формат и обработващия софтуер трябва да бъде отчетена още при проектирането.

6.2. Опростяване, изглаждане и повторна триангулация

Опростяването намалява броя на върховете и лицата, като се стреми да запази формата. Ако съобщението е свързано с конкретни върхове, тяхното премахване води до загуба на битове и нарушаване на синхронизацията. Изглаждането променя позициите на върховете спрямо техните съседи. Малките геометрични отклонения, използвани за вграждане, могат да бъдат възприети като шум и премахнати. Това въздействие е особено съществено за LSB методите. Повторната триангулация заменя съществуващите лица с нови, като запазва приблизително същата повърхност. Тя е разрушителна за методи, използващи реда на лицата, локалната топология, определени ръбове или индекси на съседни елементи.

6.2. Конвертиране и противоречие между капацитет и сигурност

При конвертиране могат да бъдат загубени нормални вектори, цветове, текстури, потребителски свойства и метаданни. Възможна е промяна на точността на координатите или на реда на елементите. Затова устойчивостта трябва да се проверява и при преобразувания като OBJ към STL или PLY към OBJ.



Фигура 4 - Опростяване на полигоналната мрежа на модела Stanford Bunny (Източник: Trevorgoodchild, Stanford bunny qem.png, Wikimedia Commons)

При увеличаване на размера на съобщението се използват повече структурни елементи. Това увеличава общото изкривяване и може да промени статистическите свойства на модела. Задачата може да се формулира като минимизиране на изкривяването при условие, че наличният капацитет е поне равен на дължината на съобщението. Адаптивните методи избират измененията според локалната сложност на мрежата. По-сложните региони прикриват промените по-добре, докато гладките области трябва да се използват ограничено. Това подобрява устойчивостта срещу стегоанализ и запазва важни геометрични характеристики [2, 3].

7 Изисквания към бъдещ стеганографски алгоритъм

7.1. Нормализиране и адаптивен избор

Преди вграждане обектът трябва да бъде приведен към определена координатна система и мащаб. Това може да намали влиянието на транслацията и равномерното мащабиране. Не всички върхове са еднакво подходящи. Върховете в гладки и визуално значими области трябва да получават по-висока цена на промяната. За предпочитане са области с по-висока геометрична сложност, където минималните изменения се различават по-трудно. Може да се въведе функция на цената $\rho i = \alpha Ci + \beta Ni + \gamma Si$, където Ci отразява изменението на локалната кривина, Ni изменението на нормалите, Si статистическата

откриваемост, а α, β и γ са тегловни коефициенти. По-ниска стойност означава по-подходящ връх.

7.2. Ключ, криптиране и контрол на грешките

Секретният ключ може да се използва за генериране на псевдослучайна последователност, която определя избраните върхове и координатни компоненти. По този начин извличането изисква притежаването на правилния ключ. Стеганографията прикрива наличието на съобщението, но не гарантира, че съдържанието му ще остане неразбираемо след откриване. Поради това тайните данни трябва да бъдат криптирани преди вграждането. Към съобщението могат да бъдат добавени контролна сума, криптографска хеш стойност, кодове за откриване и корекция на грешки или излишни копия на критичните части. Те позволяват да се провери правилността на извличането и да се възстановят част от загубените битове.

7.3. Ограничаване на изкривяването

Трябва да бъде определена максимална стойност за преместване на един връх: $\|vi - v'i\| \leq \varepsilon$, където ε зависи от размерите, резолюцията и локалната структура на модела. Еднаква стойност за всички върхове не винаги е оптимална. По-подходящо е допустимото изменение да зависи от локалната дължина на ръбовете и кривината.

Желателно е алгоритъмът да бъде колкото е възможно по-независим от реда на елементите. Върховете могат да се идентифицират чрез геометрични характеристики вместо единствено чрез индекс, макар че това създава допълнителни трудности при промени на мрежата.

8 Заключение

В настоящата статия са изследвани основни структурни елементи на цифровите 3D обекти и потенциалните възможности за тяхното използване при стеганографска защита на информация. Анализирани са координатите и последователността на върховете, лицата, топологичната свързаност, нормалните вектори, цветовете, текстурните координати и метаданните.

Резултатите показват, че координатите на върховете предлагат най-добър баланс между капацитет, незабележимост и практическа приложимост. Те присъстват във всички полигонални модели и позволяват адаптивен избор на областите за вграждане. Използването им обаче създава проблеми, свързани с квантуване, изглаждане, опростяване, геометрични преобразувания и статистическо откриване.

Последователността на върховете и лицата позволява скриване без геометрично изменение, но има ниска устойчивост при обработка. Нормалите, цветовете и текстурните координати могат да предоставят допълнителен капацитет, но приложението им зависи от формата. Метаданните не могат да осигурят достатъчно ниво на стеганографска сигурност.

Перспективен подход е разработването на адаптивен алгоритъм, който вгражда предварително криптирани данни в координатите на псевдослучайно избрани върхове. Алгоритъмът трябва да отчита локалната геометрична сложност, да ограничава изкривяването и да използва механизми за контрол и корекция на грешките.

Бъдещата работа може да включва реализиране на прототип и експерименталното му изследване върху модели с различен брой върхове и геометрична сложност. Следва да се измерят капацитетът, геометричното изкривяване, коефициентът на грешно извлечените битове и устойчивостта след основни операции за обработка.

ЛИТЕРАТУРА:

[1] Zhelezov, S., Kordov, K., Nachev, A., Stoyanova, T., Uzunova-Dimitrova, B., & Pavlova, D. (2021, November). Study of the Efficiency Coefficient of the Steganographic Embedding in Text Containers Using the Letter Replacement Method. In *2021 3rd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA)* (pp. 680-684). IEEE.

[2] Kordov, K., & Zhelezov, S. (2021). Steganography in color images with random order of pixel selection and encrypted text message embedding. *PeerJ computer science*, *7*, e380.

[3] Rafailov, R., & Paraskevov, H. (2026). Parallel Color-Specific LSB Steganography: A New Approach for Data Hiding in BMP Images. *TEM Journal*, *15*(1), 83.

[4] Zhelezov, S., Kordov, K., Nachev, A., Pavlova, D., Gindev, P., Litchkov, N., & Nesterov, K. (2024, November). A new approach for spread spectrum steganography in audio containers. In *2024 6th International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA)* (pp. 474-477). IEEE.

[5] Paraskevov, H., Valchev, G., & Rafailov, R. (2022, September). Steganographic algorithm in video with message encryption. In *AIP Conference Proceedings* (Vol. 2505, No. 1, p. 060013). AIP Publishing LLC.

[6] Surmov, D. (2025). 3D mesh watermarking using radial vertex embedding. ANNUAL OF KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, FACULTY OF MATHEMATICS AND INFORMATICS, Vol. XXVI C, 2025, pp. 41-47.

[7] Zhou, H., Zhang, W., Chen, K., Li, W., Yu, N. Three-Dimensional Mesh Steganography and Steganalysis: A Review. IEEE Transactions on Visualization and Computer Graphics, 2022. DOI: 10.1109/TVCG.2021.3072348.

[8] Zhang, Y., Zhu, J., Xue, M., Zhang, X., Cao, X. Adaptive 3D Mesh Steganography Based on Feature-Preserving Distortion. IEEE Transactions on Information Forensics and Security, 2023. DOI: 10.1109/TIFS.2023.3289313.

[9] Zhou, H., Chen, K., Zhang, W., Yao, Y., Yu, N. Distortion Design for Secure Adaptive 3-D Mesh Steganography. IEEE Transactions on Multimedia, Vol. 21, No. 6, pp. 1384–1398, 2019. DOI: 10.1109/TMM.2018.2881491.

[10] Farrag, S., Alexan, W. Secure 3D Data Hiding Technique Based on a Mesh Traversal Algorithm. Multimedia Tools and Applications, 2020. DOI: 10.1007/s11042-020-09437-w.

докторант Стоян Стоянов
ФМИ, Шуменски университет „Епископ Константин Преславски“
E-mail: s.v.stoyanov90@gmail.com