GEOMETRIK JIHATDAN MUSTAHKAM 3D SUV BELGILASH

Xudayberganov Temur Rustamovich
Abu Rayxon Beruniy nomidagi Urganch davlat universiteti Axborot xavfsizligi kafedrasi mudiri, doctordrebek@gmail.com
Kadirova Surayyo Baxodir qizi
Abu Rayxon Beruniy nomidagi Urganch davlat universiteti talabasi, surayyokadirova30@gmail.com

Annotatsiya. Geometrik jihatdan mustahkam 3D suv belgilash CAD/CAM, o‘yin sanoati va additiv ishlab chiqarish sohalarida raqamli grafik aktivlarni himoya qilishning amaliy mexanizmi hisoblanadi. Ushbu tezisda 3D suv belgilarini aniq tahdid taxminlari asosida baholash va loyihalashtirish uchun xavfsizlikka yo'naltirilgan yondashuv taqdim etiladi. Natijaviy protokol ham mustahkamlik egri chiziqlarini (hujum kuchiga nisbatan TPR/BER), ham xavfsizlik egri chiziqlarini (masalan, kuzatilgan aktivlar soniga nisbatan kalitni tiklash ustunligi) hisobga oladi. Yondashuv spektral-geometrik invariant suv belgilash misolida namoyish etiladi, bunda qayta tiklash paytidagi eigen-bazis siljishi va kalitni qayta ishlatishdagi oqish xavfi asosiy zaiflik manbalari sifatida ko'rsatiladi.

Kalit so'zlar: *3D suv belgilash, geometrik jihatdan mustahkam suv belgilash, tahdid modeli, o'yinga asoslangan xavfsizlik, oracle hujumlari, hujum taksonomiyasi, baholash protokoli.*

I. KIRISH

Uch o‘lchamli (3D) raqamli aktivlar zamonaviy iqtisodiyotning asosiy tarkibiy birligiga aylandi: mesh va nuqta bulutlari CAD/CAM tizimlarida mexanik detallarni, o'yin motorlarida qahramonlar va buyumlarni, shuningdek modellashtirish va raqamli egizaklar uchun geometriyani kodlaydi. Bitta aktiv turli formatlarga eksport qilinishi, darajaga mos variantlarga soddalashtirilishi, jismoniy obyektdan qayta skanerlanishi yoki fotosuratlardan qayta tiklanishi mumkin. Bu jarayonlar egalik huquqini himoya qilish uchun keng hujum yuzasini yaratadi. 2D tasvirlardan farqli o'laroq, 3D obyektlar faqat kichik koordinata o'zgarishlari orqali emas, balki bog'lanish (connectivity) o'zgarishlari, qayta namunalash va hatto tasvirlashni konvertatsiya qilish (mesh↔nuqta buluti↔implicit) orqali ham o'zgartirilishi mumkin.

Spektral-geometrik invariantlar (eigenqiymatlar, issiqlik/to'lqin yadrosi tasvirlagichlari) barqarorlikni ta'minlashi mumkin, ammo ularning amaliy mustahkamligi namunalash zichligi, qayta tiklash tanlovi va olish shovqiniga qattiq

bog'liq. Shu sababli xavfsizlikni baholash faqat vertex burilishlarini emas, balki olish tsikllari va diskretlashtirish siljishini ham qamrab olishi lozim. Ko'plab so'rovlarda "mustahkamlik" faqat noadaptiv o'zgarishlar ostida baholanadi va bu strategik tajovuzkorga qarshi xavfsizlikni avtomatik ravishda kafolatlamaydi — chunki u hujumlarni takrorlashi, aniqlagichlarga so'rov yuborishi yoki bir xil kalit bilan suv belgilangan ko'plab namunalardan o'rganishi mumkin.

Ushbu tezis quyidagi hissalarni qo'shadi: (i) aniq bilim, oracle kirish va foydalilik chegaralari bilan tahdid modelini belgilash; (ii) tajovuzkor maqsadlarini o'yinga asoslangan tajribalar va o'lchanadigan ustunliklar orqali formalllashtirish; (iii) tasvirlash konvertatsiyasi va olish/qayta tiklash tsikllarini o'z ichiga olgan parametrlashtirilgan hujum taksonomiyasi va takrorlanuvchi hujum kutubxonasi interfeysini taqdim etish; (iv) buzilish (distortion) metrikalari, statistik ishonch va xavfsizlik hisobotini birlashtiruvchi hisobot protokolini taklif qilish.

II. TAHDID MODELI

Suv belgilash sxemasi Π to'rt algoritmdan iborat: KeyGen, Embed, Detect va ixtiyoriy Extract. Kerckhoffs uslubidagi taxmin bo'yicha, sxemaning barcha detallari (tashuvchi tanlovi, model arxitekturasi, chegaralar) ommaviy hisoblanadi; faqat kalit k (va ixtiyoriy joylashtirish tasodifiyligi) maxfiy qolishi kerak. Bu "maxfiylik orqali xavfsizlik" prinsipidan qochishga imkon beradi.

Foydalilik cheklovi tajovuzkorning natijaviy aktivi Y dastur talablariga mos, ya'ni belgilangan chegara τ doirasida qolishini talab qiladi. Buzilish vektori $D(X,Y) = \{d_{RMS}, d_H, d_N, d_{Perc}, ...\}$ va qabul qilish predikati $U(X,Y;\tau)$ orqali "model va aktivni butunlay buzib yo'q qilish orqali olib tashlash" muvaffaqiyat sifatida hisoblanmaydi.

Tajovuzkorning kirish rejimlari to'rt turga bo'linadi: (a) oflayn — tajovuzkor faqat bitta suv belgilangan aktivni oladi; (b) tanlangan aktiv — joylashtirish xizmatidan tanlangan aktivlar uchun so'rov yuborish mumkin (suv belgilash-xizmat-sifatida modeli); (c) aniqlash oracle — Detect funksiyasiga qora quti sifatida so'rov yuborish mumkin (bozor tekshirish API'si); (d) kombinatsiyalashgan — ikkala oracle ham so'rov chegaralari (Q_E, Q_D) bilan mavjud. Bundan tashqari, tajovuzkor bir xil kalit bilan suv belgilangan q ta aktivni kuzatishi mumkin, bu esa kalit haqidagi ma'lumotning oqishiga olib keladi.

Tajovuzkor besh maqsadga ega bo'lishi mumkin: (G1) foydalilik saqlangan holda olib tashlash; (G2) qonuniy joylashtirishsiz qalbakilashtirish; (G3) noaniqlik — bir necha egalik da'vosining qabul qilinishi; (G4) foydali yukni manipulyatsiya qilish; (G5) kalitni tiklash. Minimal hisobot uchun talab etiladigan parametrlar: xavfsizlik parametri λ, foydalilik chegarasi τ, kuzatilgan namunalar soni q, joylashtirish-oracle so'rovlari Q_E, aniqlash-oracle so'rovlari Q_D va hisoblash byudjeti B.

III. O'YINGA ASOSLANGAN XAVFSIZLIK TA'RIFLARI

Har bir tajovuzkor maqsadi o'lchanadigan tajriba ("o'yin") sifatida ifodalanadi. To'g'rilik (benign mustahkamlik) o'yini noadversar o'zgarish oilasi ostida aniqlash ehtimoli kamida $1-\varepsilon$ bo'lishini talab qiladi.

- Olib tashlash o'yini (G_remove): tajovuzkor X^{ω} ni oladi va Y ni chiqaradi; g'alaba shartlari — Detect(Y,k)=0 va U(X,Y;τ)=1. Ustunlik: Adv_remove(A) = Pr[g'alaba].
- Qalbakilashtirish o'yini (G_forge): tajovuzkor X^{ω} olmasdan Y ni chiqaradi; g'alaba — Detect(Y,k)=1.
- Noaniqlik o'yini (G_amb): bir necha kalit $k_1,...,k_n$ mavjud bo'lganda, tajovuzkor kamida ikki kalit uchun ijobiy aniqlanishga erishsa g'alaba qozonadi.
- Kalitni tiklash o'yini (G_key): tajovuzkor q ta namunani kuzatib, k ga teng kuchga ega bo'lgan taxmin $\hat{k}$ ni chiqaradi; ustunlik Adv_key(q) q ning o'sishi bilan kuzatishga asoslangan oqish sababli ortishi kutiladi.
- Foydali yukni manipulyatsiya qilish o'yini (G_msg, ixtiyoriy): Detect(Y,k)=1 bo'lsa-da, Extract(Y,k) chiqargan xabar asl xabardan farq qilsa, tajovuzkor g'alaba qozonadi.

Detect funksiyasi ball s(Y,k) asosida bo'lganda, barqaror yolg'on signal darajasi α ta'minlash uchun chegara t_α tozalik nazorat namunalari asosida belgilanadi va barcha hujumlar davomida o'zgarmas saqlanadi. Bu jadval shaklida quyidagicha umumlashtiriladi: olib tashlash → Adv_remove; qalbakilashtirish → Adv_forge (t_α darajasida); noaniqlik → Adv_amb; kalitni tiklash → Adv_key(q); foydali yuk buzilishi → buzilish darajasi.

IV. HUJUM TAKSONOMIYASI VA BAHOLASH PROTOKOLI

Har bir hujum operatori A_θ aktivni o'zgartiradi va parametrlarni θ sifatida qayd etadi. Sakkiz toifa taklif etiladi: (A) o'xshashlik transformatsiyalari (aylanish, siljish, masshtab); (B) geometriya filtrlash (Laplasian/Taubin silliqlash, keskinlashtirish, kvantlash); (C) shovqin va uchqunlar (Gauss shovqini, normal siljishi); (D) bog'lanish hujumlari (soddalashtirish, qayta meshlash, subdivizatsiya); (E) qisman tahrirlar (kesish, patch almashtirish, teshik to'ldirish); (F) olish/qayta tiklash (nuqta bulutiga qayta namunalash, skaner shovqini, Poisson qayta tiklash); (G) tasvirlashni konvertatsiya qilish (mesh↔nuqta buluti↔voksel/implicit); (H) moslashuvchan hujumlar (ball minimallashtirish, oracle yordamida qidiruv, o'rganilgan olib tashlagichlar).

Har bir operator sof funksiya sifatida aniqlanadi: $Y = A_\theta(X; \text{urug'})$, meta = (A, θ, urug', versiya). Amaliy piratlik holatlarida bir necha operator ketma-ket qo'llaniladi (kompozitsion hujum), masalan: soddalashtirish → qayta meshlash → silliqlash → qayta tiklash, va bu foydalilik cheklovi $U(X, \bar{A}(X); \tau)=1$ va hisoblash byudjeti B doirasida amalga oshiriladi.

Baholash protokoli to'qqiz bosqichdan iborat: (1) topologiya va geometriya bo'yicha xilma-xil ma'lumotlar to'plamini tanlash; (2) kalit siyosatini (aktiv-bo'yicha, egasi-bo'yicha yoki umumiy) hisobotga kiritish; (3) joylashtirish kuchini τ_embed bilan kalibrlash; (4) belgilangan yolg'on signal darajasi α da qat'iy chegara t_α ni sozlash; (5) hujum jadvalini bajarish va metama'lumotlarni qayd etish; (6) TPR(θ), BER(θ), buzilish D(X,Y) va vaqt/xotira metrikalarini hisoblash; (7) belgilangan t_α da Adv_remove, Adv_forge, Adv_amb va Adv_key(q) ni baholash; (8) bootstrap ishonch intervallari orqali statistik ishonchni ta'minlash; (9) minimal hisobot ro'yxatini (ma'lumotlar, kalitlar, chegara, hujumlar, foydalilik, natijalar, xavfsizlik) taqdim etish.

XULOSA

Ushbu tezisda geometrik jihatdan mustahkam 3D suv belgilashni moslashuvchan tajovuzkorlarga qarshi xavfsizlik bilan birgalikda baholash zarurligi asoslab berildi. 3D aktivlar desinxronizatsiya va diskretlashtirish siljishiga alohida moyil, chunki tajovuzkorlar faqat vertex koordinatalarini emas, balki bog'lanish, namunalash zichligi va tasvirlashning o'zini ham o'zgartirishi mumkin. Shu sababli, cheklangan sondagi odatiy qayta ishlash operatsiyalariga bardosh berish bozor va 3D bosib chiqarish piratligi sharoitlarida real himoyaning yetarli dalili emas.

Kerckhoffs uslubidagi tahdid modeli, o'yinga asoslangan xavfsizlik ta'riflari, parametrlashtirilgan hujum taksonomiyasi va takrorlanuvchi hujum kutubxonasi interfeysi, shuningdek foydalilik cheklovlarini kuchaytiruvchi va ishonch intervallari bilan mustahkamlik egri chiziqlarini nashr etuvchi baholash va hisobot protokoli taklif etildi. Spektral-geometrik invariant suv belgilash uchun xavfsizlik tahlili sxemasi eigen-bazis siljishi va kalitni qayta ishlatishdagi oqishni asosiy xavf manbalari sifatida belgiladi. Kelajakda xavfsizlikka yo'naltirilgan hisobot 3D suv belgilash tadqiqotlari va joriy etilishi uchun standart talabga aylanishi lozim, chunki egalik dalili faqat hujum ostida ishonchli qolgandagina va aktiv foydaliligini saqlab qolgandagina qadr-qiymatga ega bo'ladi.

ADABIYOTLAR

1. J. Djumanov, T. Khudayberganov, T. Turdiyev, I. Nafasov, J. Uralov, "Robustness of Spectral–Geometric Invariants Under Realistic 3D Acquisition Distortions: A Critical Review, Taxonomy, and Comparative Evaluation Protocol," IEEE EDM 2026, 2026.
2. K. Wang, G. Lavoué, F. Denis, A. Baskurt, "A Comprehensive Survey on Three-Dimensional Mesh Watermarking," IEEE Transactions on Multimedia, vol. 10, no. 8, pp. 1513–1527, 2008.
3. K. Wang, G. Lavoué, F. Denis, A. Baskurt, X. He, "A Benchmark for 3D Mesh Watermarking," in Proc. Shape Modeling International Conference (SMI), 2010, pp. 231–235.

4. F. Cayre, C. Fontaine, T. Furon, "Watermarking Security Part I: Theory," in Security, Steganography, and Watermarking of Multimedia Contents VII, vol. 5681, 2005, pp. 746–757.
5. M. Kazhdan, M. Bolitho, H. Hoppe, "Poisson Surface Reconstruction," in Eurographics Symposium on Geometry Processing (SGP), 2006, pp. 61–70.