ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտ

Ատենախոսություն

Ինֆորմացիոն-տեսական մեթոդների կիրառությունը թվային պատկերների որակի գնահատման և մասնավոր ինֆորմացիայի պաշտպանության խնդիրներում

Մաստոյան Կարեն Արթուրի

Ե.13.05 մաթեմատիկական մոդելավորում, թվային մեթոդներ եվ ծրագրերի համալիրներ մասնագիտությամբ
տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի համար

Գիտական ղեկավար՝ ֆիզ մաթ գիտ դոկտոր, պրոֆ
Մարիամ Եվգենիի Հարությունյան

Երևան 2025

ՆԵՐԱԾՈՒԹՅՈՒՆ

Թեմայի արդիականությունը

21-րդ դարում թվային տեխնոլոգիաների և արհեստական բանականության (ԱԲ) առաջընթացը էապես ազդել է տվյալների մշակման և կիրառման գործընթացներ և առաջ է բերել մի շարք խնդիրներ, որոնք սպասում են իրենց լուծումներին: Թվային պատկերների որակի գնահատման ու անձնական տվյալների պաշտպանության ոլորտներում նույնպես առկա են կենսական կարևորություն ունեցող խնդիրներ: Հրատապությունը պայմանավորված է տեխնոլոգիական հնարավորությունների ընդլայնմամբ և դրանց հետ կապված անվտանգության ու գաղտնիության խախտումների աճով:

Թվային պատկերները կիրառվում են գիտական հետազոտությունների, բժշկական պատկերների ախտորոշման, արհեստական բանականության ուսուցման, հեռահաղորդակցության և այլ ոլորտներում: Սակայն պատկերների որակը հաճախ տուժում է տարբեր աղավաղումների հետևանքով, օչինակ գունավոր աղմուկը, բլուրացումը, սեղմման արդյունքում առաջացող աղավաղումները և այլն: Այս իրավիճակներում կարևոր է պատկերի որակի օբյեկտիվ գնահատումը, որը հնարավորություն կտա.

- բարձրացնել պատկերների սեղմման և վերականգնման արդյունքում որակի կորստի վերլուծության ճշգրտությունը,
- ընտրել մեքենայական ուսուցման համար պահանջվող որակի մակարդակի պատկերներ,
- խուսափել առողջապահական կամ անվտանգության ոլորտներում սխալ որոշումներից՝ պայմանավորված պատկերների թերի որակով:

Գրականության մեջ կիրառվում են որակի գնահատման մի շարք չափանիշներ, ինչպիսիք են PSNR-ը (peak signal-to-noise ratio), SSIM-ը (կառուցվածքային նմանության ինդեքս) և այլ մեծություններ: Սակայն այդ մեծություններն ունիվերսակ չեն և կատարյալ չեն, այսինքն ոչ բոլոր կիրառություններում են արդյունավետ:

Այդ պատճառով բաց խնդիր է գտնել այնպիսի որակի գնահատման մեծություններ, որոնք արդյունավետ են տարբեր աղավաղումների դեպքում:

Մասնավոր տվյալների պաշտպանությունը ստացել է նոր կարևորություն՝ պայմանավորված մեծ տվյալների (Big Data) աճով և դրանց հետ աշխատող համակարգերի (օրինակ՝ առողջապահական ռեգիստրներ, սոցիալական մեդիա հարթակներ և էլեկտրոնային կառավարման համակարգեր) զարգացմամբ: Գենետիկ տվյալների վերլուծության և առողջապահական պատկերների հետ աշխատող ԱԲ կիրառությունների աճն ընդգծում է անձնական տվյալների պաշտպանության կարևորությունը: Առանց համապատասխան մեթոդների, այս ոլորտները կարող են դառնալ ոչ միայն տվյալների չարաշահման, այլև մարդկային էթիկայի խախտման հարթակներ:

Հավաքագրվող տվյալների վերլուծությունները պահանջում են դրանց հրապարակումը առանց գաղտնագրման, ինչը կարող է հանգեցնել զգայուն ինֆորմացիայի արտահոսքին, այսինքն անձնական գաղտնիության խափանմանը:

Գրականությունում առկա են մի շարք մոտեցումներ [հղում DP, anonimization], ինչպիսիք են անանունացումը, գաղտնագրական մեթոդները, որոնք ոչ բոլոր կիրառություններում են ընդունելի, որոնք չեն լուծում ոլորտի բոլոր խնդիրները:

Թվային պատկերների որակի և գաղտնիության ապահովման հարցերը հաճախ կապված են միմյանց հետ: Օրինակ՝ բարձր որակով բժշկական պատկերների պահպանումը և փոխանցումը պահանջում է ինչպես որակի ապահովում, այնպես էլ ինֆորմացիայի պաշտպանություն:

Այսպիսով, վերը նշված արդիական խնդիրները պահանջում են գիտական լուծումներ՝ ունենալով կիրառական մեծ կարևորություն: Ինֆորմացիոն տեսական

մոտեցումները ապացուցել են, որ կարող են էական ներդրում ունենալ նշված խնդիրների լուծմանը հասնելու համար:

Աշխատանքի հիմնական նպատակը և դիտարկված խնդիրները

Աշխատանքի հիմնական *նպատակն* է մշակել նոր մոտեցումներ թվային պատկերների որակի գնահատման և անձնական տվյալների պաշտպանության ոլորտներում բաց խնդիրների լուծման համար:

Այդ նպատակին հասնելու համար ինֆորմացիայի տեսության գործիքակազմի ներդրմամբ դիտարկվել են հետևյալ խնդիրները:

1. Առաջարկել պատկերների որակի գնահատման չափանիշ՝ արդյունավետ տարբեր աղավաղումների դեպքում՝ հիմնվելով այլ չափանիշների և մարդկային տեսողական համակարգի (Human Visual System) համեմատության վրա:
2. Հետազոտել մասնավոր ինֆորմացիայի պաշտպանության խնդիրները և լուծման մեթոդները և առաջարկել նոր մոտեցումներ:
3. Դիտարկել էլեկտրոնային քվեարկության համակարգում մասնավոր ինֆորմացիայի գաղտնիության և ստուգելիության իրարամերժ պրոբլեմը՝ տալով գործուն լուծումներ:

Հետազոտության օբյեկտները

Ատենախոսության շրջանակում հետազոտության օբյեկներ են խոշոր կազմակերպությունների կողմից թողարկված դիֆերենցիալ գաղտնիության գրադարանները, թվային աղավաղված պատկերները՝ մասնավորապես TID2013 տվյալների հենքը, դրանց համեմատման չափանիշները, էլեկտրոնային քվեարկության համակարգերը և դրանց անվտանգային բնութագրիչները:

Հետազոտության մեթոդները

Ատենախոսության արդյուքները հիմնված են ինֆորմացիայի տեսության մեթոդների վրա, կիրառելով էնտրոպիայի և փոխադարձ ինֆորմացիայի գաղափարները, դիֆերենցիալ գաղտնիության մեթոդը: Կիրառական արդյունքները հենված են դեմքի ճանաչման մեթոդի վրա, ծրագրային մշակումների վրա python ծրագրավորման լեզվով և որոշ գրադարաններով:

Պաշտպանությանը ներկայացվող հիմնական դրույթները

1. Կատարվել է համապարփակ վերլուծություն ինֆորմացիայի տեսության գործիքների և մեթոդների կիրառման արդյունավետության վերաբերյալ մասնավոր ինֆորմացիայի պաշպանության խնդիրներում: Հետազոտվել է դիֆերենցիալ գաղտնիության կիրառությունը Google-ի, IBM-ի գրադարաններում, Apple ընկերությունում և R փաթեթում:
2. Առաջարկվել է որպես պատկերի որակի գնահատման չափման մեծություն դիտարկել նորմալացված փոխադարձ ինֆորմացիան, որի արդյունավետությունը հիմնավորվել է փորձարկումների և այլ մեծությունների հետ համեմատման միջոցով:
3. Միավորելով պատկերների ճանաչման և մասնավոր ինֆորմացիայի պաշտպանության մոտեցումները՝ առաջարկվել է լուծում գաղտնիություն և ստուգելիություն իրարամերժ պրոբլեմի էլեկտրոնային քվեարկության համակարգերում:

Գիտական նորույթը

Նորմալացված փոխադարձ ինֆորմացիան (Normalized Mutual Information, NMI) առաջին անգամ է առաջարկվել աղավաղված պատկերների համեմատման չափանիշ:

Էլեկտրոնային քվեարկության նույնականացման համար կիրառված դեմքի պատկերի գաղտնիության ապահովումը լուծվել է հիմնվելով էնտրոպիայի հատկությունների վրա, որը լիովին նոր մոտեցում է:

Կիրառական նշանակությունը

Մշակվել է ծրագրային համակարգ՝ Python լեզվով, որը թույլ է տալիս ներմուծել աղավաղված պատկերների հենքերը, թվային պատկերների որակի գնահատման և համեմատության իրականացման համար՝ տարբեր չափերի կիրառմամբ: Ծրագրային ապահովումը թույլ է տալիս ճկուն կերպով կարգավորել գնահատման պարամետրերը՝ հնարավորություն տալով ստացված արդյունքներն արտահանել CSV կամ Excel ֆայլային ձևաչափերով՝ հետագա վերլուծության և ներկայացման համար: Համակարգի ճարտարապետությունը նախատեսված է նաև ընդլայնման համար, ինչը թույլ կտա նոր մեթոդների և տվյալների հենքերի ինտեգրում՝ հետագա հետազոտությունների համար:

Էլեկտրոնային քվեարկության համակարգում մշակվել է ծրագրային հատված, որը թույլ է տալիս իրականացնել քվեարկողի պատկերի էնտրոպիայի հաշվարկ, պատկերների պիքսելների պատահական խառնում:

Ստացված արդյունքների գրաքննությունը և փորձարկումը

Ատենախոսության արդյուքները զեկուցվել են՝

- Գավառի պետական համալսարանի ամենամյա՝ 24-րդ (2021 թ.), 25-րդ (2022 թ.), 26-րդ (2023 թ.), 27-րդ (2024թ.) գիտաժողովներին,
- CSIT «Data Analytics and Mathematical Modeling» միջազգային աշխատաժողովում, Վրաստան 2024,
- Industry 4.0, IX International scientific conference, Վառնա, Բուլղարիա 2024:

Աշխատանքի արդյունքները քննարկվել են ՀՀ ԳԱԱ ԻԱՊԻ ընդհանուր սեմինարին:

Հրապարակումները

1. M. Haroutunian, K. Mastoyan, The Role of Information Theory in the Field of Big Data Privacy, Mathematical Problems of Computer Science vol. 55, pp. 35–43, 2021. doi: 10.51408/1963-0071
2. K. Mastoyan, Differential Privacy in Practice: Use Cases, Mathematical Problems of Computer Science vol. 56, pp. 48–55, 2021. doi: 10.51408/1963-0078
3. M. Haroutunian, D. Asatryan, K. Mastoyan, Analyzing the Quality of Distorted Images by the Normalized Mutual Information Measure, Mathematical Problems of Computer Science vol. 61, pp. 7–14, 2024. doi: 10.51408/1963-0111
4. M. Haroutunian, K. Mastoyan, A. Margaryan, A simple e-voting system ensuring identification, privacy and verifiability, INDUSTRY 4.0 vol. 1/20, ISSN - 2535-0153, 150-153, 2024.
5. M. Haroutunian, K. Mastoyan, A. Margaryan, New Approach for Online Voting Ensuring Privacy and Verifiability, ISSN 0361-7688, Programming and Computer Software, vol. 50, Suppl. 1, pp. S60–S68, 2024. doi: 10.1134/S0361768824700427