ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Մաստոյան Կարեն Արթուրի

ԻՆՖՈՐՄԱՑԻՈՆ-ՏԵՍԱԿԱՆ ՄԵԹՈԴՆԵՐԻ ԿԻՐԱՌՈՒԹՅՈՒՆԸ ԹՎԱՅԻՆ ՊԱՏԿԵՐՆԵՐԻ ՈՐԱԿԻ ԳՆԱՀԱՏՄԱՆ և ՄԱՍՆԱՎՈՐ ԻՆՖՈՐՄԱՑԻԱՅԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ԽՆԴԻՐՆԵՐՈՒՄ

Ե.13.05 - «Մաթեմատիկական մոդելավորում, թվային մեթոդներ և ծրագրերի համալիրներ» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի համար

ՍԵՂՄԱԳԻՐ

Երևան 2025

INSTITUTE FOR INFORMATICS AND AUTOMATION PROBLEMS OF THE NAS RA

Mastoyan Karen

APPLICATION OF INFORMATION-THEORETICAL METHODS IN THE PROBLEMS OF DIGITAL IMAGE QUALITY ASSESSMENT AND PRIVACY

ABSTRACT

of the dissertation for obtaining a Ph.D. degree in Technical Sciences on specialty 05.13.05 “Mathematical modelling, numerical methods and program complexes”

Yerevan 2025

Ատենախոսության թեման հաստատվել է ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում:

Գիտական ղեկավար՝ ֆիզ. մաթ. գիտ. դոկտոր. Մ. Ե. Հարությունյան

Պաշտոնական ընդդիմախոսներ՝ ֆիզ. մաթ. գիտ. դոկտոր Հ. Ա. Սահակյան

տեխ. գիտ. թեկնածու Վ. Կ. Ավետիսյան

Առաջատար կազմակերպություն՝ Հայաստանի ազգային պոլիտեխնիկական համալսարան

Ատենախոսության պաշտպանությունը տեղի կունենա 2025թ. փետրվարի 27-ին ժամը 14:00-ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Ինֆորմատիկա» մասնագիտական խորհրդի նիստում հետևյալ հասցեով՝ Երևան, 0014, Պ. Սևակի 1:

Ատենախոսությանը կարելի է ծանոթանալ ՀՀ ԳԱԱ ԻԱՊԻ գրադարանում:

Սեղմագիրն առաքված է 2025 թ.-ի հունվարի 27-ին:

Մասնագիտական խորհրդի գիտական

քարտուղար ֆիզ. մաթ. գիտ. դոկտոր՝ Մ. Ե. Հարությունյան

The topic of the dissertation was approved at the Institute of Informatics and Automation Problems of NAS RA.

Scientific supervisor: M. E. Harutyunyan, D. Ph. M. S.
Official opponents: H. A. Sahakyan, D. Ph. M. S.
V. K. Avetisyan, Ph.D.
Leading organization: National Polytechnic University of Armenia

The Defense will take place on 27 February 2025; at 14:00, at the Specialized Council 037 "Informatics" at the Institute of Informatics and Automation Problems of NAS RA. Address: Yerevan, 0014, P. Sevak 1.

The Dissertation is available at the library of IIAP NAS RA.

The abstract is delivered on 27 January, 2025.

Scientific Secretary of the Specialized Council, D.Ph.M.S. M. E. Haroutunian

Աշխատանքի ընդհանուր նկարագիրը

Թեմայի արդիականությունը

21-րդ դարում թվային տեխնոլոգիաների և արհեստական բանականության (ԱԲ) առաջընթացն էապես ազդել է տվյալների մշակման և կիրառման գործընթացներին 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, օրինակ 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 ունիվերսալ 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, ինչպիսիք են անանունացումը, գաղտնագրական մեթոդները, որոնք ոչ բոլոր կիրառություններում են ընդունելի և 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 հետազոտել ինֆորմացիայի տեսության դերը թվային պատկերների որակի գնահատման և անձնական տվյալների պաշտպանության ոլորտներում և մշակել նոր մոտեցումներ բաց խնդիրների լուծման համար:

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

1. Հետազոտել մասնավոր ինֆորմացիայի պաշտպանության խնդիրները և լուծման մեթոդները և առաջարկել նոր մոտեցումներ:
2. Առաջարկել պատկերների որակի գնահատման չափանիշ՝ արդյունավետ տարբեր աղավաղումների դեպքում՝ հիմնվելով այլ չափանիշների և մարդկային տեսողական համակարգի (Human Visual System) համեմատության վրա:
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:

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:

Հրապարակումներ

Ատենախոսության հիմնական արդյուքները հրապարակվել են 5 գիտական աշխատություններում, որոնց ցանկը բերված է սեղմագրի վերջում:

Աշխատանքի ծավալը և կառուցվածքը

Ատենախոսության ծավալը կազմում է 101 էջ, բաղկացած է ներածությունից, 4 գլուխներից, եզրակացությունից, օգտագործված գրականության ցանկից, որը ներառում է 91 գրականության հղումներ:

Աշխատանքի բովանդակությունը

Ներածություն բաժնում հիմնավորվում է ատենախոսության արդիականությունը, ձևակերպված է աշխատանքի նպատակը, դիտարկված խնդիրները, գիտական նորույթը, կիրառական նշանակությունը և պաշտպանության ներկայացված հիմնական դրույթները:

Առաջին գլուխը ունի ներածական բնույթ: Կատարվել է գրականության վերլուծություն, հետազոտվել են խնդիրները և բերված են ինֆորմացիայի տեսության հիմնական տարրերը, մասնավորապես՝ աշխատանքում կիրառված են X պատահական մեծության *Էնտրոպիան*, որը անորոշության չափն է, տրվում է հետևյալ բանաձևով.[1]

$$H(X) = -\sum_{l=1}^{L} p(x_l) \log p(x_l),$$

X, Y պատահական մեծությունների փոխադարձ ինֆորմացիան

$$I(X \wedge Y) = -\sum_{x}\sum_{y} p(x,y) \log p(x,y):$$

Շատ կիրառություններում տարբեր մեծություններ համեմատելու համար դիտարկվում են փոխադարձ ինֆորմացիայի նորմալացված տարբերակներ: Առաջին գլխում դիտարկվել են տարբեր մոտեցումներ և հիմնավորված ընտրվել է հետևյալ հեռավորության չափը

$$NMI = 1 - \frac{I(X \wedge Y)}{\max\{H(X),H(Y)\}}, \qquad (2)$$

քանի որ այն բավարարում է մետրիկայի բոլոր հատկություններին, օգտագործում է փոխադարձ ինֆորմացիայի առավել խիստ վերին սահմանը max{H(X)H(Y)}: Այս մեծությունը կիրառվել է դասակարգման (classification) և խմբավորման (clustering) խնդիրներում, սակայն չի դիտարկվել որպես պատկերների որակի գնահատման մեծություն:

Մեծ Տվյալներում մասնավոր ինֆորմացիայի պաշտպանության խնդիրների ուսումնասիրությունը գտնվում է զարգացման նախնական փուլում: Չնայած մշակվել են մի շարք մեխանիզմներ, այդ թվում՝ գաղտնագրական լուծումներ և անանունացման մոտեցումներ, մասնավոր տվյալների պաշտպանությունը դեռևս մարտահրավեր է մնում:

Այս գլխում հիմնավորվել է նաև, որ ինֆորմացիայի տեսության մոտեցումները կարևոր ներդրում կարող են ունենալ մասնավոր ինֆորմացիայի պաշտպանության և թվային պատկերների որակի գնահատման ոլորտների արդիական խնդիրներում:

Երկրորդ գլուխը նվիրված է մասնավոր ինֆորմացիայի պաշտպանության (privacy) խնդիրների և մեթոդների հետազոտմանը: Մեծ տվյալների հետ աշխատելիս մասնավոր ինֆորմացիայի պահպանումը հետազոտության արագ աճող ոլորտ է: Մասնավոր ինֆորմացիայի պահպանման առաջին մոտեցումն անանունության մեթոդն էր: Վերջին ուսումնասիրությունները ցույց են տվել, որ պարզապես անանուն տվյալների շտեմարանները կարող են հեշտությամբ ենթարկվել հարձակման գաղտնիության տեսանկյունից: Հետագայում առաջարկվեց դիֆերենցիալ գաղտնիությունը (ԴԳ), որն ապացուցեց, որ ամենահեռանկարայինն է: Գաղտնիության և հրապարակված տվյալների օգտակարության միջև փոխզիջումը, ինչպես նաև այլ հարցերի, ինչպիսիք են

[1] Cover T. M., Thomas J. A., Elements of Information Theory, 2nd edition, Wiley-Interscience, 2006.

անանունության հասնելու տարբեր եղանակները համեմատելու համար չափի առկայությունը ընկնում է ինֆորմացիայի տեսության տիրույթում: Չնայած գրականության մեջ մի շարք ակնարկային հոդվածների առկայությանը, ինֆորմացիայի տեսության մեթոդների հնարավորությունները պատշաճ ուշադրության չէին արժանացել:

Այս գլխում, մասնավորապես, ներկայացված է [1] հոդվածում իրականացված հետազոտությունը, որտեղ վերլուծվել են ինֆորմացիայի տեսության գործիքների և մեթոդների միջոցով լուծված մասնավոր ինֆորմացիայի պահպանման տարաբնույթ խնդիրներին նվիրված մի շարք հրապարակումներ:

Հետազոտվել է ԴԳ տեսությունը, ինչպես նաև խոշոր ընկերությունների կողմից մշակված լուծումները [2]: Մասնավորապես, ուսումնասիրվել է Apple-ի, Google-ի, IBM-ի կողմից ԴԳ իրականացման տարբերակները, ինչպես նաև Benjamin I. P. Rubinstein-ի կողմից R-ի համար մշակված փաթեթը: Արդյունքում կարող ենք նշել, որ Apple-ը ակտիվորեն օգտագործում է ԴԳը իր համակարգերում, սակայն բաց կոդով գրադարաններ չի տրամադրում: Google-ի գրադարանը հարմար է C++, Go, Java ծրագրավորման լեզուներով գրված սկրիպտերի համար և թույլ է տալիս իրականացնել մի շարք ալգորիթմներ, ինչպիսիք են Laplace մեխանիզմը, Gaussian մեխանիզմը, ցրվածքի (Variance) և ստանդարտ շեղման (Standard deviation) հաշվարկները և այլն: IBM-ի ԴԳ գրադարանը գրված է Python լեզվով և առավել հարմար է օգտագործել Python միջավայրում:

Rubinstein-ի diffpriv փաթեթը թույլ է տալիս R լեզվով իրականացնել ԴԳ պրոցեսը, որը բաց է տարբեր միջավայրերի և ալգորիթմների համար: Սույն ուսումնասիրությունը օգտակար է նոր ԴԳ կիրառություններ և գրադարաններ մշակելու համար:

Երրորդ գլխում արտացոլված են [3] հոդվածում հրապարակված արդյունքները: ՈՒսումնասիրվել է, թե ինչպես են տարբեր տեսակի աղավաղող ալգորիթմներն ազդում պատկերի որակի ամբողջական գնահատման վրա ստուգանմուշի օգտագործմամբ, հատկապես, երբ ներառված են սուբյեկտիվ որակի գնահատականները: Առաջարկվել է որպես պատկերների համեմատման չափանիշ դիտարկել NMI -ը (2): Արդյունքները համեմատվում են պատկերի որակի գնահատման համար Վեյբուլի բաշխման վրա հիմնված W^2 արդյունքների, հայտնի PSNR նմանության չափի և MOS-ի հետ:

3. 1 բաժնում կատարվել է գրականության վերլուծություն և հիմնավորվել է հետազոտության նպատակը:

3. 2-ը նվիրված է պատկերների որակի գնահատման (ՊՈԳ) գործընթացի հետազոտմանը, հիմնական մեթոդաբանություններին, դասերին և հիմնական գործոններին: ՈՒսումնասիրվել է TID2013 տվյալների հենքը[2], որն ընդգրկում է 3000 պատկեր՝ աղավաղված 24 տեսակի ալգորիթմներով և MOS գնահատականներով:

Այս հետազոտության մեջ առաջարկվել է պատկերի որակի գնահատման նոր մոտեցում՝ օգտագործելով NMI հասկացությունը[3]: NMI-ն հաշվում է ինֆորմացիայի քանակը հղման և

[2] Ponomarenko N., Jin L., Ieremeiev O., Lukin V., Egiazarian K., Astola J., Vozel B., Chehdi K., Carli M., Battisti F., et al., "Image database TID2013," Signal Processing: Image Communication, vol. 30, pp. 57–77, 2015.

[3] Kraskov A., Stogbauer H., Andrzejak R. G., Grassberger P., "Estimating mutual information," Phys. Rev. E, v. 69, 2004

աղավաղված պատկերների միջև: NMI տեսական հիմքերը գալով ինֆորմացիայի տեսությունից, տալիս է ամուր և լավ սահմանված հիմք պատկերի հեռավորությունը չափելու համար: Ավելին, սանդղակային ինվարիանտությունը դարձնում է NMI-ն կիրառելի տարբեր լուծաչափերի պատկերների համար: Հաջորդիվ, դրա ոչ պարամետրային բնույթի շնորհիվ չի պահանջում նախնական ենթադրություններ պատկերի տվյալների մասին՝ բարձրացնելով նրա ադապտացվողականությունը տարբեր տեսակի պատկերների համար:

3. 3 բաժնում դիտարկվել և համեմատվել են հետևյալ մեծությունները:

Mean Opinion Score (MOS)

MOS-ը սուբյեկտիվ չափի մեծություն է, որը ներկայացնում է մարդկային դիտորդների միջին կարծիքը: Այն օգտակար է մյուս չափանիշների գնահատման համար:

Peak Signal-to-Noise Ratio (PSNR)

PSNR-ը լայնորեն կիրառվող չափման մեծություն է պատկերի որակի գնահատման համար՝ հաճախ կիրառվելով պատկերի մշակման և սեղմման ոլորտում: Այն գնահատում է պատկերի իսկությունը՝ համեմատելով ազդանշանի առավելագույն ուժը (սկզբնական պատկեր) աղմուկի ուժի հետ (ներառված ներկայացման ընթացքում, սովորաբար Գաուսյան աղմուկ):

Թերություններ. Այն հաճախ չի արտացոլում մարդկային ընկալման նրբությունները և կարող է ոչ բոլոր ազդանշանների կամ սեղմման տեխնիկայի համար հարմար լինել: PSNR-ը պիքսելային մակարդակի վրա հիմնված հաշվարկ է, որն անտեսում է տեղայնացված կամ կառուցվածքային աղավաղումների նկատմամբ մարդու տեսողական զգայունությունը: Այն հատկապես թույլ է գլոբալ լուսավորության շեղումների, գունային շեղումների և բլոկային աղավաղումների հայտնաբերման գործում: Արդյունքում, այն հաճախ չի արտացոլում մարդու սուբյեկտիվ գնահատականը, հատկապես երբ առկա են խիստ տեսանելի, բայց չափով փոքր աղավաղումներ:

W^2 (Structural Similarity Metric)

W^2-ը պատկերի որակի չափի մեծություն է, որը գնահատում է կառուցվածքային նմանությունը սկզբնական պատկերի և Գաուսյան աղմուկ ավելացված պատկերի միջև:

Այս չափի մեծությունը հիմնված է պատկերի գրադիենտային մագնիտուդի Վեյբուլի բաշխման մոդելի վրա, որի խտությունը տրված է հետևյալ բանաձևով՝

$$f(x;\lambda,\eta) = \frac{\eta}{\lambda}\left(\frac{x}{\lambda}\right)^{\eta-1} exp\left[-\left(\frac{x}{\lambda}\right)^{\eta}\right], x \geq 0,$$

որտեղ $\eta>0$ ձևի պարամետրն է, իսկ $\lambda>0$՝ սանդղակի պարամետրը: Բաշխման պարամետրերը գնահատվում են բոլոր գրադիենտների մեծությունների ամբողջականության հիման վրա՝ օգտագործելով Սոբել օպերատորը:

Երկու պատկերների նմանությունը (մոտությունը) գնահատվում է Weibull բաշխման պարամետրերի գնահատականների մոտությամբ՝ հետևյալ բանաձևով՝

$$W^2 = \frac{min(\eta_1,\eta_2)min(\lambda_1,\lambda_2)}{max(\eta_1,\eta_2)max(\lambda_1,\lambda_2)}:$$

Հետազոտությունը[4] ցույց է տվել, որ այս չափի մեծությունը զգայուն է այն աղավաղումների տեսակների նկատմամբ, որոնք ազդում են պատկերի կառուցվածքին և բովանդակությանը:

Նորմալացված փոխադարձ ինֆորմացիա (NMI)

Այս հետազոտության մեջ առաջարկվում է դիտարկել (2) սահմանված NMI հեռավորության չափի մեծությունը: NMI արժեքները տատանվում են 0-ից 1-ի միջև, որտեղ 0-ն մատնանշում է կատարյալ նմանություն, իսկ 1-ը՝ նմանության բացակայություն: Ինֆորմացիայի տեսությունից բացի, NMI-ն լայնորեն օգտագործվում է նաև պատկերի համադրման, պատկերի հատվածավորման և այլ կիրառությունների մեջ[5]:

NMI-ն հաճախ կիրառվում է խմբավորման ալգորիթմները գնահատելու կամ նույն տվյալների տարբեր խմբերի համեմատության համար: Այն հիմնված է ինֆորմացիայի տեսության սկզբունքների վրա, ինչը տալիս է տեսական հիմք և հարմար է տարբեր ոլորտներում, ինչպիսիք են մեքենայական ուսուցումը, նմուշի ճանաչումը և տվյալների պեղումը:

Մշակվել է ծրագրային փաթեթ և կատարվել են փորձարկումներ, որոնց արդյունքներն արտացոլված են **3.4 բաժնում:**

Ընտրված տվյալների հենքը TID2013-ն է: Այս տվյալների հենքը պարունակում է 3000 պատկեր, որոնք ստացվել են 25 սկզբնական պատկերներից՝ աղավաղված 24 տարբեր տեսակների միջոցով, յուրաքանչյուրն ունենալով հինգ մակարդակ: Տվյալների հենքի հեղինակները լայնածավալ փորձ են անցկացրել պատկերների որակի վիզուալ գնահատման համար՝ միավորային համակարգի կիրառմամբ, ներգրավելով տարբեր երկրների մեծ թվով մասնակիցներ: Այս տվյալների մշակման արդյունքում յուրաքանչյուր 3000 պատկերին տրամադրվել է թվային MOS միավոր:

Փորձարկումների համար 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: Բոլոր անհրաժեշտ քանակները հաշվարկվել են մշակված ծրագրային համակարգի միջոցով, և արդյունքները ներմուծվել են Excel աղյուսակներում: Հիմնական տվյալներն են՝ արդյունքները կապված սկզբնական և հինգ աղավաղված նմուշների հետ տվյալ պատկերի համար:

Յուրաքանչյուր տվյալների հավաքածուի համար կիրառվել են երեք գնահատման մեթոդներ՝ NMI, PSNR, W2, և դրանք համեմատվել են MOS-ի հետ: Այս մեթոդները օգտագործվել են տվյալների հենքի պատկերների որակի գնահատման և վերլուծության

[4] Asatryan D., Haroutunian M., Sazhumyan G., Hakobyan G., "Procedure for an alyzing the quality, structure and subjective rating of distorted images by the Full Reference technique", Intern. Scientific Journals of Scientific Technical Union of Me chanical Engineering "Industry 4.0", Mathematical Modeling, vol. 6, no. 4, pp. 100-102, 2022.

[5] Ruiz F. E., Pérez P. S., Bonev B. I., Information theory in computer vision and pattern recognition, Springer, 2009.

համար:

Մի շարք սցենարներում NMI-ն ցուցադրել է համանման զգայունություն՝ համեմատած այլընտրանքային չափանիշների հետ: Օրինակ, նկ. 3. 2-ում ցուցադրված են Additive noise in color աղմուկի հինգ մակարդակներ: Բոլոր չափման մեծությունների արժեքները յուրաքանչյուր մակարդակի համար ներկայացված են աղյուսակ 3.1-ում:

Նկ. 3. 2. Additive noise in color 5 մակարդակները TID2013 տվյալների հենքից. Պատկեր թիվ 15

Աղյուսակ 3.1. TID2013 տվյալների հենքի 15-րդ պատկերի փորձարարական արդյունքները (Additive noise in color)

NMI	PSNR	W^2	MOS
0.14	42.33	0.87	6.09
0.17	39.45	0.78	5.82
0.22	36.47	0.66	5.64
0.27	33.61	0.53	4.89
0.34	31.39	0.38	4.64

Որոշ դեպքերում NMI-ն ցուցադրում է ավելի բարձր արդյունավետություն: Օրինակ՝ Non eccentricity pattern noise աղմուկի մեթոդով աղավաղման դեպքում W^2 արժեքները մոտ են մեկին, ինչը նշանակում է, որ այն ցածր արդյունք է ցուցադրում մարդկային գնահատման և ընկալման տեսանկյունից, մինչդեռ NMI արժեքները մոտ են մարդկային գնահատմանը (աղյուսակ 3.2, նկ. 3.3):

Նկ. 3.3. Չաղավաղված պատկեր և 5-րդ մակարդակի աղավաղված պատկեր (Non eccentricity pattern noise)

Աղյուսակ 3.2. 8-րդ պատկերի փորձարկման արդյունքները TID2013 տվյալների հենքից (Non eccentricity pattern noise)

NMI	PSNR	W2	MOS
0.06	43.33	1	5.65
0.10	41.30	1	5.43
0.16	39.08	0.99	4.87
0.20	37.82	0.99	4.75
0.24	36.92	0.99	4

TID2013-ում առկա են տարբեր աղավաղումներ, որոնց դեպքում NMI-ն սովորաբար տալիս է ավելի լավ համընկնում մարդու սուբյեկտիվ ընկալման հետ, քան PSNR-ը: Օրինակ, Contrast change (Աղավաղում 17) և Mean shift (intensity shift) (Աղավաղում 16) աղավաղումները ներառում են գլոբալ լուսատվության կամ կոնտրաստի շեղումներ, որոնք PSNR-ը գնահատում է պիքսելային մակարդակի միջին քառակուսային սխալով, ինչի հետևանքով նույնիսկ փոքր, բայց համընդհանուր փոփոխությունները կարող են շեշտակիորեն նվազեցնել դրա արժեքը, մինչդեռ մարդու աչքը նման գլոբալ շեղումների հանդեպ նույնքան զգայուն չէ: Ի հակադրություն, NMI-ն վերլուծում է պատկերի պիքսելային բաշխումն ու փոխադարձ ինֆորմացիան, ինչի շնորհիվ այն ավելի կայուն է նմանատիպ գլոբալ փոփոխությունների դեպքում, և եթե պատկերի հիմնական կառուցվածքը պահպանվում է, NMI-ն մնում է համեմատաբար բարձր ու լավագույնս արտացոլում է սուբյեկտիվ գնահատականը: Նույն տրամաբանությամբ, Color saturation change (Աղավաղում 18) և Chromatic aberrations (Աղավաղում 23) աղավաղումները պարունակում են գունային շեղումներ, որոնք PSNR-ը հաճախ չի ներկայացնում ըստ ընկալման իրական չափորոշիչների, քանի որ այն կամ RGB բաղադրիչները դիտարկում է առանձին, կամ ընդհանրապես աշխատում է միայն լուսային (grayscale) մակարդակի վրա: Մինչդեռ NMI-ն կարող է որսալ գունային միաժամանակյա կապերը, ուստի գույնի նույնիսկ փոքր շեղումները, որոնք մարդու աչքին ակնհայտ են, ավելի մատչելի են դարձնում NMI-ի միջոցով ստացվող գնահատականը: Բացի այդ, Masked noise (Աղավաղում 4), Spatially correlated noise (Աղավաղում 3) և Non-eccentricity pattern noise (Աղավաղում 14) աղավաղումները, որոնք ունեն ոչ համասեռ կամ տարածականորեն շաբլոնավորված բնույթ, PSNR-ի մոտ կարող են «չերևալ» որպես մեծ խնդիր, քանի որ այն հաշվարկում է ընդհանուր միջին սխալը, մինչդեռ տեղայնացված արատները մարդու աչքի համար կարող են շատ անհանգստացնող լինել: Ընդհակառակը, NMI-ն գնահատում է ընդհանուր պատկերի վիճակագրական բաշխումը, և երբ աղմուկը կենտրոնացած է որոշ հատվածներում կամ ձևավորվում է որոշակի շաբլոնով, փոխադարձ ինֆորմացիան միանգամայն փոխվում է, ինչն ավելի լավ է համընկնում դիտորդների MOS-ի հետ: Նույնը վերաբերում է նաև Local block-wise distortions

(Աղավաղում 15), JPEG compression (Աղավաղում 10) և JPEG2000 compression (Աղավաղում 11) աղավաղումներին, որտեղ block-based կամ wavelet-based մեթոդները հաճախ առաջացնում են զանգվածային, բայց տեսողականորեն առանձին հատվածներում նկատվող արատներ, որոնք PSNR-ի տեսանկյունից կարող են չհանգեցնել մեծ սխալի, եթե այդ արատները զբաղեցնում են պատկերի միայն փոքր մասը: Այնինչ NMI-ն գրանցում է պատկերի բաշխման և պիքսելների հարաբերությունների փոփոխությունը, ինչի հետևանքով նույնիսկ քիչ տարածք ունեցող, բայց տեսանելի փաստը կարող է ազդեցություն ունենալ գնահատականի վրա: Gaussian blur (նկ. 3. 4) (Աղավաղում 8)-ի դեպքում էլ (աղ 3. 3) մեղմ աղոտացումը PSNR-ի արժեքը էապես չի նվազեցնում, քանի որ միջին քառակուսային սխալը մեծ չէ, բայց մարդկային ընկալման մեջ եզրագծերի և կարևոր դետալների կորուստը շատ ավելի կարևոր է, իսկ NMI-ի շնորհիվ փոխադարձ ինֆորմացիան նվազում է, գերազանցապես արտացոլելով հենց այդ տեսողական ընկալումը: Այս ամենն ընդգծում է, որ NMI-ն, լինելով բաշխման և ինֆորմացիայի վրա հիմնված մոտեցում, հաճախ ավելի լավ է համընկնում մարդու սուբյեկտիվ գնահատման հետ, քան PSNR-ը, հատկապես երբ խոսքը գնում է գունային շեղումների, գլոբալ լուսատվության և կոնտրաստի փոփոխությունների, տեղայնացված արատների, ինչպես նաև աղոտացման կամ այլ տեսակի աղավաղումների մասին, որոնք մարդու աչքը նկատում է ավելի ուժեղ, քան ցույց է տալիս սովորական պիքսելային մակարդակի սխալը:

Աղյուսակ 3.3. 6-րդ պատկերի փորձարկման արդյունքները TID2013 տվյալների հենքից (Gaussian blur)

NMI	PSNR	*W2*	MOS
0,204	35,032	0,84	5,189
0,299	32,342	0,72	4,583
0,404	30,901	0,54	3,485
0,492	30,162	0,32	2,702
0,564	29,578	0,19	2,054

Նկ. 3.4. Չաղավաղված պատկեր և 5-րդ մակարդակի աղավաղված պատկեր (Gaussian blur)

NMI առավելություններից մեկն էլ կայանում է նրանում, որ այն նորմալացված մեծություն է և տարբեր աղավաղումների մակարդակները համեմատվում են 0-1 միջակայքում:

Այսպիսով ստուգանմուշի օգտագործմամբ ուսումնասիրվեց, թե ինչպես են տարբեր տեսակի աղավաղող ալգորիթմներն ազդում պատկերի որակի ամբողջական գնահատման վրա, հատկապես, երբ ներառված են սուբյեկտիվ որակի գնահատականները: Կիրառվել է TID2013 տվյալների հենքը, որը պարունակում է 3000 պատկեր, որոնք աղավաղված են 24 տարբեր ալգորիթմներով, MOS-ի հետ համատեղ: Համեմատվել են NMI արդյունքները պատկերի որակի գնահատման համար Վեյբուլի բաշխման վրա հիմնված W^2 արդյունքների, հայտնի PSNR նմանության չափի և MOS ի հետ: Արդյունքում փորձարկումներով հիմնավորվեց, որ NMI-ը կարող է ավելացվել պատկերի որակի գնահատման չափման մեծությունների ցանկում:

Չորրորդ գլխում հետազոտվել է մասնավոր ինֆորմացիայի պաշտպանության խնդիրն էլեկտրոնային քվեարկության (է-քվեարկություն, e-voting) համակարգերում: Այստեղ խնդիրը բարդանում է, եթե պահանջ է դրվում ապահովել ստուգելիությունը, քանի որ այդ երկու պահանջները իրարամերժ են: Առաջարկվել է նոր մոտեցում, որը լուծում է այդ պրոբլեմը առանց բարդ գաղտնագրական մեթոդների, օգտագործելով միայն դեմքի ճանաչումը, պատկերի էնտրոպիայի հատկությունները և հեշ ֆունկցիաները [4], [5]:

4.1 բաժնում քննարկված են է-քվեարկության առավելությունները, անվտանգային խնդիրները, ինչպես նաև վերջին տարիների հետազոտությունները:

Այսպիսով, մի կողմից է-քվեարկությունը պոտենցիալ օգուտներ է պարունակում քվեարկության արդյունավետության և մատչելիության բարելավման գործընթացում, բայց մյուս կողմից ներկայացնում է զգալի մարտահրավերներ, որոնք պետք է դիտարկվեն՝ ապահովելու անվտանգությունը, ամբողջությունը և ընտրությունների արդարությունը:

Մեծ թվով հրապարակումներ են նվիրված է-քվեարկության համակարգերի խնդիրների հետազոտմանը: Մասնավորապես, վերջին տարիների ակնարկ հոդվածներն իրենց հերթին հղվում են հրապարակումների մեծ ցանկի վրա:

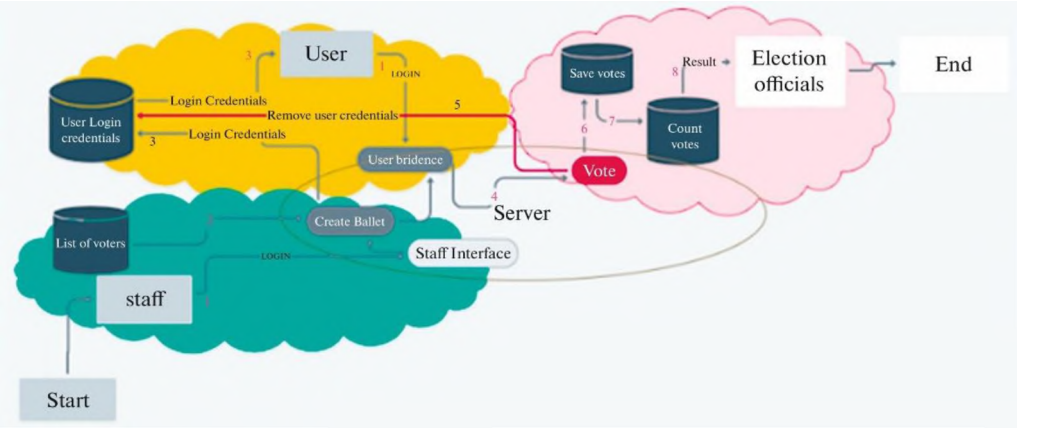
Է-քվեարկության համակարգին ներկայացվող պահանջները դիտարկված են **4. 2 բաժնում**: Մասնավորապես, անվտանգության հիմնական բնութագրերն են.

- *Նույնականացում կամ իրավասություն:* Ապահովել, որ միայն իրավասու ընտրողները կարողանան քվեարկել:
- *Ամբողջականություն*: Ապահովել, որ քվեները գրանցվում են այնպես, ինչպես արվել են, և հաշվարկվեն այնպես, ինչպես գրանցվել են:
- *Կայունություն:* Որևէ քվեաթերթիկ չպետք է փոփոխվի սերվերում պահվելուց հետո:
- *Մասնավոր ինֆորմացիայի պաշտպանություն:* Ապահովել, որ ընտրողի և նրա քվեարկության միջև կապ չլինի, այլ կերպ ասած, քվեարկողի մասին ինֆորմացիան լինի պաշտպանված:
- *Անանունություն*: Քվեաթերթիկները պետք է լինեն իրարից չտարբերակվող:
- *Գաղտնիություն:* Պաշտպանել քվեի բովանդակությունը չթույլատրված անձանցից:
- *Սրտուգելիություն:* Հնարավորություն տալ ընտրողներին ստուգել, որ իրենց քվեն ճիշտ է հաշվարկվել՝ առանց անանունությունը խաթարելու:

- *Մեկանգամյա քվեարկություն*: Տվյալ ընտրողը կարող է քվեարկել միայն մեկ անգամ, թույլ չտալ որևէ ընտրողի քվեարկել ավելի քան 1 անգամ:

Բավականին բարդ է համակարգ կամ արձանագրություն ստեղծելը, որը կբավարարի բոլոր պահանջներին: Օրինակ՝ մարտահրավեր է ընտրողների գաղտնիությունը պահպանելը, բայց միևնույն ժամանակ ապահովելը քվեների ստուգելիությունը: Հետևաբար, անհրաժեշտ են մշտական հետազոտություններ և բարելավումներ:

Հաջորդ **4. 3 բաժինը** նվիրված է առցանց ընտրական համակարգի կառուցվածքին:



Գործընթաց 1.

- Մուտք աշխատակազմի կողմից (Login): Պահանջում է անվտանգ կառավարել քվեարկության համակարգի ադմինիստրատիվ հասանելիությունը:

- Նույնականացման մեթոդները կարող են ներառել՝ կենսաչափական նույնականացում (օր.՝ մատնահետք կամ դեմքի ճանաչում), պետական փաստաթղթերի նույնականացում կամ եզակի մուտքի հավատարմագրեր:

Գործընթաց 2.

- Քվեաթերթիկի ստեղծում (Ballot Creation): Համակարգը պետք է տրամադրի մեխանիզմ՝ անուններ, կուսակցական պատկանելություններ և այլ համապատասխան տվյալներ ստեղծելու և կառավարելու համար:

- Ինֆորմացիայի գաղտնիությունը պետք է երաշխավորվի այս փուլում:

- Քվեաթերթիկը պետք է ձևավորվի հականալի և հեշտ կիրառելի:

Գործընթաց 3.

- Մուտքի տվյալների փոխանցում (Transmission of Login Credentials) ընտրողներին:

-Պահանջում է ապահովել ընտրողների ցուցակի ճշգրտությունը և անվտանգությունը, ինչպես նաև կանխել չարտոնված հասանելիությունն ու մանիպուլյացիան:

Գործընթաց 4.

-Նույնականացվելուց հետո ընտրողը ստանում է հնարավորություն քվեարկելու:

Գործընթաց 5.

- Համակարգը պետք է ստուգի ընտրողի իրավասությունը և ապահովի, որ անձի տվյալները հեռացվեն քվեաթերթիկից՝ պահպանելով ընտրողի անանունությունը և բացառեն կրկնությունը:

Գործընթաց 6.

- Համակարգը գրանցում է քվեներն ապահովելով կայունությունը և մասնավոր ինֆորմացիայի պաշտպանությունը:

Գործընթաց 7.

- Քվեարկության ժամկետը ավարտվելուց հետո համակարգը հաշվում է ձայները և գեներացնում արդյունքները՝ ապահովելով ամբողջականությունը: Այս գործընթացը կարող է ներառել քվեների հավաքագրումը, անոմալիաների հայտնաբերումը և առաջացած այլ խնդիրների լուծումը:

Գործընթաց 8.

- Պետք է ապահովվի արդյունքների ճշգրիտ գրանցում:

Վերջապես, է-քվեարկության համակարգի նկատմամբ վստահությունը բարձրացնելու նպատակով հարկավոր է ներմուծել ստուգելիության մեխանիզմներ:

4. 4 բաժնում դիտարկված են գոյություն ունեցող գաղտնագրական լուծումները: Դրանցից են անհամաչափ գաղտնագրումը, հանրային բանալիով գաղտնագրումը, հոմոմորֆ կոդավորումը, հեշ ֆունկցիաները, զրոյական գիտելիքի ապացույց մեթոդը և այլ տեխնիկաներ:

4. 5 բաժնում ներկայացված է նույնականացման, մասնավոր ինֆորմացիայի պաշտպանության և ստուգելիության առաջարկված նոր լուծումը և կայունության ապացույցը: Մոտեցումը օգտագործում է Շենոնի էնտրոպիայի չափը, մասնավորապես այն հատկության շնորհիվ, որ պատկերի պիքսելների խառնումը չի փոխում աղավաղված պատկերի էնտրոպիան:

Առցանց քվեարկության գործընթացում մենք առաջարկում ենք օգտագործել *դեմքի ճանաչումը* ընտրողների նույնականացման համար: Հիմնական պահանջը դեմքի ճանաչման մոդելի ընտրությունն է, որը պետք է լինի ճշգրիտ և ի վիճակի կառավարել մեծ թվով ճանաչման հարցումներ՝ ապահովելով հարթ քվեարկության գործընթաց:

Առաջարկվող է-քվեարկության համակարգում ենթադրում ենք, որ ընտրողների ցանկը ներառում է նրանց ID քարտերը դեմքի պատկերներով: Գործընթաց 3-ում անձնակազմը նամակ է ուղարկում յուրաքանչյուր ընտրողին քվեարկության մասին տեղեկությամբ և է-քվեարկության համակարգի ինտերֆեյսի հղումով: Հղումը բացում է ընտրողի վավերացման էջը, որն իրականացվում է դեմքի ճանաչման միջոցով: Համակարգը կհամեմատի անձի դեմքը ID քարտի դեմքի պատկերի հետ և կստուգի ընտրողի իրավասությունը: Երբ դեմքը ճանաչվի, օգտագործողի դեմքի պատկերն անմիջապես խառնվում է պատահական ձևով (նկ. 4.2): Պատկերի էնտրոպիան H-ն ուղարկվում է ընտրողի էլեկտրոնային փոստին: Հակառակ դեպքում, մուտքը մերժվում է:

Նկ. 4.2. Հիմնական պատկերը և խառնված պատկերը նույն պիքսելների փոխակերպմամբ ունեն նույն էնտրոպիան H = 7.862951331478429

Վավերացումից հետո ընտրողը կարող է էլեկտրոնային ձևով կատարել իր քվեարկությունը (գործընթաց 4): Էլեկտրոնային քվեարկության արդյունքը լրացված ընտրաթերթիկն է խառնված պատկերի հետ, այսինքն՝ անանունացված ընտրաթերթիկը (նկ. 4.3):

Նկ. 4.3. Անանունացված ընտրաթերթիկ

Երբ ընտրողը հաստատում է իր քվեարկությունը, լրացված ընտրաթերթիկի խառնված պատկերի h1 հեշ արժեքը (գործընթաց 5) ուղարկվում է ընտրողի էլեկտրոնային փոստին: Քվեարկությունը տվյալ անձի համար փակվում է, որպեսզի տեղի չունենա կրկնակի քվեարկություն:

Գործընթաց 6-ում համակարգը խառնված դեմքի պատկերով քվեն արձանագրում է տվյալների հենքում: Միևնույն ժամանակ տվյալների հենքում գտնվող ցանկի h2 հեշ արժեքը ուղարկվում է ընտրողի էլեկտրոնային փոստին:

Այժմ քննարկենք առաջարկվող գործընթացների **անվտանգության, գաղտնիության և ստուգելիության** կողմերը:

Ընտրողի դեմքի պատկերի կամ խառնված պատկերի էնտրոպիան կլինի ընտրողի նույնացուցիչ համարը: Այն կարելի է համարել եզակի թիվ, քանի որ, մի կողմից, այն չի կարող կրկնվել անգամ նույն անձի համար (եթե անգամ թույլատրելի լիներ), իսկ մյուս կողմից, քանի որ էնտրոպիան 16 թվանշանից բաղկացած թիվ է (նկ. 4.2-ում H=7.862951331478429), հետևաբար կարող է ունենալ մոտ 10^{16} տարբեր արժեքներ, ինչը շատ ավելին է, քան հնարավոր ընտրողների քանակը:

Ինչպես ասվեց, համակարգում օգտագործվող էնտրոպիան կամ նույնացուցիչ համարն

անփոփոխ է պատկերի պիքսելների ցանկացած տեղափոխության համար: Ապացուցենք, որ խառնված պատկերը երաշխավորում է ընտրողի գաղտնիությունը, քանի որ գործնականում անհնար է խառնված պատկերից ստանալ բնօրինակ պատկերը: Իսկապես, դիտարկենք հետևյալ 5×5=25 պիքսել ունեցող պատկերի օրինակ, ապա հնարավոր տեղափոխությունների քանակը հավասար է P!=25!, որը մոտ 10^{24}-ի կարգի թիվ է: Հայտնի է, որ 1 տարին հավասար է 31536000 վայրկյան, որը ավելի մեծ է քան $3x10^7$: Եթե սուպերհամակարգիչը կարողանա ստուգել մեկ փոխադրություն 10^{-10} վայրկյանում, ապա 10^7 տարի է պահանջվելու, որպեսզի գտնվի բնօրինակ պատկերը: Բայց իրական պատկերը կարող է ավելի շատ պիքսելներ ունենալ: Նկ. 4.2-ում դիտարկվող պատկերը 1024×1024=10485761024 պիքսել ունի, հետևաբար հնարավոր տեղափոխությունների թիվը աստղաբաշխականորեն մեծ է:

Երբ պիքսելները պատահականորեն են խառնվում, գործընթացը սովորաբար ոչ դետերմինացված է և չի պահպանում բնօրինակ դիրքերի մասին որևէ հիշողություն: Խառնված պատկերում յուրաքանչյուր պիքսելի դիրքը անկախ է դրա նախնական դիրքից, եթե լրացուցիչ տեղեկատվություն (օրինակ՝ տեղադրության բանաձև կամ բանալի) չի պահպանվում: Սա հաշվարկի առումով անհնարին է դարձնում առանց ճշգրիտ տեղափոխությունը իմանալու շրջել պիքսելների խառնումը: Այս ամենը դեռ հաշվի չի առնում, որ յուրաքանչյուր պիքսել ունի 3 բաղադրիչ, որոնք նույնպես կարող են տեղափոխվել: Հետևաբար, ապացուցեցինք, որ պատահականորեն խառնված պատկերը շրջել դեպի բնօրինակ վիճակն անհնար է առանց լրացուցիչ տվյալների կամ փոխադրությունների գրանցման:

Քվեարկության ավարտին յուրաքանչյուր ընտրող հնարավորություն կունենա ստուգելու քվեարկությունը՝ ուղարկելով հարցում իր նույնացուցիչ համարով (պատկերի էնտրոպիա): Համակարգը կստուգի այդ համարի գոյությունը, կհաշվի համապատասխան քվեի h1 հեշ արժեքը և նախորդ ցանկի h2 հեշ արժեքը, ապա կուղարկի ընտրողին: Եթե բոլոր ընդունված հեշ արժեքները համընկնեն նախկինում էլեկտրոնային փոստով ստացված արժեքների հետ, ապա դա նշանակում է, որ

- ընտրողի ընտրաթերթիկը չի անտեսվել կամ ջնջվել (ամբողջականություն),
- քվեն ճիշտ է արձանագրված (կայունություն),
- քվեների ցանկը չի փոփոխվել (լիարժեքություն):

Հակառակ դեպքում, եթե h1-ի կամ h2-ի արժեքները փոփոխված են, ընտրողը կարող է արձանագրել խարդախությունը:

Առաջարկվող լուծումներն իրականացվել են, մշակված է-քվեարկության համակարգը կոչվել է SiVote, որի կառուցվածքը և իրականացման մանրամասները ներկայացված են **4. 6 բաժնում:**

1. SiVote համակարգի տեխնիկական ճարտարապետությունը հիմնված է ժամանակակից վեբ տեխնոլոգիաների վրա՝ ապահովելով անվտանգ, հուսալի և թափանցիկ քվեարկության գործընթաց:

2. Docker-ը կիրառվում է ծրագրային համակարգի տեղակայման համար, ինչը հնարավորություն է տալիս ճկուն կիրառումներ ինչպես ամպային հարթակներում (օր.՝ Hetzner, Amazon), այնպես էլ տեղական սերվերներում:

3. Ամպային ծառայություններն օգտագործվում են միայն անհրաժեշտության դեպքում՝ ապահովելով տվյալների պահման համապատասխանությունը երկրի ներսում:

Համակարգի նախատիպը մշակվել է օգտագործելով **Django**, որը բարձր մակարդակի Python վեբ շրջանակ է՝ նախատեսված արագ մշակման և մաքուր, պրագմատիկ դիզայնի համար: Django-ն ընտրվել է իր ամրության, մասշտաբայնության և հարուստ գրադարանների էկոհամակարգի համար: Այն ապահովում է գերազանց անվտանգություն, որը կարևոր է զգայուն քվեարկության տվյալների մշակման համար: Django-ի **ORM (Object Relational Mapping)**-ը MySQL-ի հետ ապահովում է արդյունավետ տվյալների կառավարում և մշակում, ինչը կարևոր է քվեարկության գրառումները և steganography-ի մետատվյալները պահպանելու համար:

Հիմնական հնարավորություններն են՝

- ներկառուցված նույնականացման և անվտանգության հատկություններ,
- մասշտաբայնություն՝ մեծ քանակի քվեարկության գրառումների համար,
- արդյունավետ ORM՝ տվյալների հենքի հետ փոխազդեցությունների համար:

Django-ն SiVote-ում կատարում է օգտատերերի նույնականացում, երթուղում և սերվերային տրամաբանության կառավարում:

MySQL տվյալների հենքը ընտրվել է իր հուսալիության, բարձր արտադրողականության և օգտագործման հարմարավետության համար: Աջակցում է բարդ հարցումներին, որոնք անհրաժեշտ են տվյալների կառավարման արդյունավետության համար: Ապահովում է մասշտաբայնություն և անվտանգություն, ինչը backend-ի համար իդեալական ընտրություն է: **Nginx**-ը հանդես է գալիս որպես վեբ սերվեր՝ ապահովելով ստատիկ ֆայլերի գերազանց արտադրողականություն և անվտանգություն: **Gunicorn**-ը կառավարում է Django հավելվածները և վեբ հարցումները: **Տեղակայման փուլում** Django-ն կարգավորվում է վեբ սերվերի և տվյալների հենքի կապի համար անհրաժեշտ կարգավորումներով: **SMTP ծառայությունը** ինտեգրվում է նամակներ ուղարկելու համար:

Քվեաթերթիկի ձևավորման մոդուլը թույլ է տալիս ադմինիստրատորներին ստեղծել տարբեր տեսակի քվեաթերթիկներ: Այս քվեաթերթիկները կարող են ներառել մեկ ընտրության տարբերակներ, բազմակի ընտրության տարբերակներ, վանդակներ և այլ հատուկ ընտրանքներ, որոնք հարմար են տարբեր տեսակի ընտրությունների կամ հարցումների համար: Այս ճկունությունն երաշխավորում է, որ համակարգը կարող է տեղավորել քվեարկության սցենարների լայն շրջանակ: Դինամիկ քվեաթերթիկները պահվում են JSON ձևաչափով՝ ծրագրային ապահովման ֆունկցիոնալ փոփոխություններ չպահանջելու համար:

Դեմքի ճանաչումը օգտագործում է Python-ի **OpenCV, dlib և PIL** գրադարանները՝ իրական ժամանակում նույնականացման գործընթացում: **OpenCV.** Հզոր համակարգչային տեսողության գործառույթներ, որոնք կարևոր են դեմքի ճանաչման և պատկերի մշակման առաջադրանքների համար:

Պիքսելների խառնման և էնտրոպիայի հաշվարկի մոդուլը իրականացնում է պատկերի պիքսելների խառնումը պատահականացման ալգորիթմով: **Հեշավորման ալգորիթմը** հիմնված SHA-256 ալգորիթմի վրա:

Առավելություններ. Պարզ օգտագործման և միևնույն ժամանակ անվտանգ

համակարգ: Չի պահանջում վստահելի անձինք կամ գաղտնի բանալիների փոխանակում: Հարմար է լայն կիրառությունների համար և չի պահանջում գաղտնագրական գիտելիքներ:

Այսպիսով առաջարկվող է-քվեարկության համակարգը հեշտ օգտագործելի է և միևնույն ժամանակ ապահով է, հարմար է տարբեր ընտրությունների համար և հարմարվող տարբեր դեպքերի, կարող է օգտագործվել տարբեր տեսակի ընտրությունների համար: Այն չի պահանջում վստահելի անձինք և չի պահանջում գաղտնի բանալիների փոխանակում: Այն շատ պարզ է օգտվողների համար, չի պահանջում գաղտնագրման իմացություն և, հետևաբար, կարող է օգտագործվել մարդկանց լայն շրջանակի կողմից՝ առանց նախնական ուսուցման: Մասնավոր ինֆորմացիայի պաշտպանությունն ու ստուգելիությունը, ինչպես նաև այն փաստը, որ վերջնական արդյունքները գաղտնագրված չեն և հասանելի են բոլոր ընտրողների համար, վստահություն են հաղորդում այս համակարգին:

Աշխատանքի հիմնական արդյունքները

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:[1,2]

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]

3. Միավորելով պատկերների ճանաչման և մասնավոր ինֆորմացիայի պաշտպանության մոտեցումները՝ առաջարկվել է լուծում գաղտնիություն և ստուգելիություն իրարամերժ պրոբլեմի էլեկտրոնային քվեարկության համակարգերում: [4,5]

Հրապարակված աշխատանքների ցանկ

1. M. Haroutunian, K. Mastoyan, The Role of Information Theory in the Field of Big Data Privacy, Mathematical Problems of Computer Science 55, 35–43, 2021. doi: 10.51408/1963-0071
2. K. Mastoyan, Differential Privacy in Practice: Use Cases, Mathematical Problems of Computer Science 56, 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 61, 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 Volume 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, 2024, Vol. 50, Suppl. 1, pp. S60–S68. © Pleiades Publishing, Ltd., 2024. doi: 10.1134/S0361768824700427

ПРИМЕНЕНИЕ ИНФОРМАЦИОННО-ТЕОРЕТИЧЕСКИХ МЕТОДОВ В ЗАДАЧАХ ОЦЕНКИ КАЧЕСТВА ЦИФРОВОГО ИЗОБРАЖЕНИЯ И ЗАЩИТЫ ЧАСТНОЙ ИНФОРМАЦИИ

Абстракт

В XXI веке развитие цифровых технологий и искусственного интеллекта (ИИ) существенно повлияло на сферу обработки и применения данных и породило ряд проблем, которые ждут своего решения. Также актуальны вопросы в области оценки качества цифровых изображений и защиты персональных данных. Актуальность обусловлена расширением технологических возможностей и ростом связанных с ними нарушений безопасности и конфиденциальности.

Цифровые изображения используются в научных исследованиях, диагностике медицинских изображений, обучении ИИ, телекоммуникациях и других областях. Однако качество изображения часто страдает от различных искажений, таких как цветовой шум, размытость, искажения в результате сжатия и т. д. В этих ситуациях важна объективная оценка качества изображения, которая позволит:

- повысить точность анализа потери качества в результате сжатия и восстановления изображений,
- отбирать изображения необходимого уровня качества для машинного обучения,
- избегать принятия неправильных решений в сфере здравоохранения или безопасности из-за низкого качества изображения.

В литературе используется ряд критериев оценки качества, таких как PSNR (пиковое отношение сигнала к шуму), SSIM (индекс структурного сходства) и другие величины. Однако эти величины не являются универсальными и не являются идеальными, т. е. они не эффективны во всех приложениях.

Поэтому остается открытой проблема поиска величин оценки качества, которые эффективны в случае различных искажений.

Конфиденциальность приобрела новое значение в связи с ростом Больших данных и развитием систем, которые работают с ними (например, реестры здоровья, платформы социальных сетей и системы электронного управления). Рост приложений ИИ, работающих с генетическими данными и изображениями здоровья, подчеркивает важность конфиденциальности. Без соответствующих методов эти области могут стать площадками не только для неправомерного использования данных, но и для нарушения человеческой этики.

Анализ собранных данных требует их публикации без шифрования, что может привести к утечке конфиденциальной информации, т. е. нарушению личной конфиденциальности.

В литературе существует ряд подходов, таких как анонимизация, криптографические методы, которые не являются приемлемыми во всех приложениях и не решают всех проблем в этой области.

Вопросы обеспечения качества и конфиденциальности цифровых изображений часто связаны друг с другом. Например, хранение и передача высококачественных медицинских изображений требует как обеспечения качества, так и защиты информации.

Таким образом, вышеупомянутые актуальные проблемы требуют научных решений, имеющих большое практическое значение. Информационно-теоретические подходы доказали, что они могут внести значительный вклад в достижение решения указанных проблем.

Основная цель работы и задачи

Основная цель работы — исследовать роль теории информации в областях оценки качества цифровых изображений и защиты персональных данных и разработать новые подходы к решению открытых задач.

Для достижения этой цели были рассмотрены следующие задачи с использованием инструментов теории информации.

1. Исследовать задачи защиты частной информации и методы их решения и предложить новые подходы.

2. Предложить критерий оценки качества изображения, эффективный при различных искажениях, на основе сравнения с другими критериями и зрительной системой человека.

3. Рассмотреть конфликтную проблему конфиденциальности и проверяемости частной информации в системе электронного голосования, предложив эффективные решения.

Объем и структура работы

Объем диссертации составляет 101 страниц, состоит из введения, 4 глав, заключения и списка использованной литературы, который включает 91 ссылку.

Основные результаты работы

1. Проведен комплексный анализ эффективности использования инструментов и методов теории информации в задачах конфиденциальности. Изучено использование дифференциальной конфиденциальности в библиотеках Google, IBM, Apple и пакете R. [1, 2]

2. Предлагается рассматривать нормализованную взаимную информацию как меру оценки качества изображения, эффективность которой обоснована экспериментами и сравнением с другими величинами. [3]

3. Путем объединения подходов распознавания изображений и защиты конфиденциальности предлагается решение проблемы компромисса конфиденциальности и проверяемости в системах электронного голосования. [4, 5]

APPLICATION OF INFORMATION-THEORETICAL METHODS IN THE PROBLEMS OF DIGITAL IMAGE QUALITY ASSESSMENT AND PRIVACY

Abstract

In the 21st century, the advancement of digital technologies and artificial intelligence (AI) has significantly affected the field of data processing and applications and has given rise to a number of problems that are waiting for their solutions. There are also vital issues in the areas of digital image quality assessment and personal data protection. The urgency is due to the expansion of technological capabilities and the growth of security and privacy violations associated with them.

Digital images are used in scientific research, medical image diagnostics, artificial intelligence training, telecommunications and other fields. However, image quality often suffers from various distortions, such as color noise, blurring, distortions resulting from compression, etc. In these situations, an objective assessment of image quality is important, which will allow:

- to increase the accuracy of the analysis of quality loss as a result of image compression and restoration,
- to select images of the required quality level for machine learning,
- to avoid wrong decisions in the health or security sectors due to poor image quality.

A number of quality assessment criteria are used in the literature, such as PSNR (peak signal-to-noise ratio), SSIM (structural similarity index), and other quantities. However, these quantities are not universal and are not perfect, i.e., they are not effective in all applications.

Therefore, it is an open problem to find quality assessment quantities that are effective in the case of various distortions.

Privacy has gained new importance due to the growth of Big Data and the development of systems that work with them (e.g., health registries, social media platforms, and electronic governance systems). The growth of AI applications working with genetic data and health images emphasizes the importance of privacy. Without appropriate methods, these areas can become platforms not only for data misuse, but also for violations of human ethics.

The analysis of collected data requires their publication without encryption, which can lead to the leakage of sensitive information, i.e., the violation of personal privacy.

There are a number of approaches in the literature, such as anonymization, cryptographic methods, which are not acceptable in all applications and do not solve all the problems of the field.

The issues of ensuring the quality and confidentiality of digital images are often related to each other. For example, the storage and transmission of high-quality medical images requires both quality assurance and information protection.

Thus, the above-mentioned current problems require scientific solutions, having great practical importance. Information theoretical approaches have proven that they can make a significant contribution to achieving the solution of the mentioned problems.

The main goal of the work and the considered problems

The main goal of the work is to investigate the role of information theory in the fields of digital image quality assessment and personal data protection and to develop new approaches for solving open problems.

To achieve this goal, the following problems were considered with the employment of information theory tools.

1. Investigate the problems of private information protection and solution methods and propose new approaches.

2. Propose an image quality assessment criterion that is effective in the case of various distortions, based on a comparison with other criteria and the Human Visual System.

3. Consider the conflicting problem of privacy and verifiability of private information in the electronic voting system, providing effective solutions.

Scope and structure of the work

The volume of the dissertation is 101 pages, consists of the introduction, 4 chapters, conclusion and the list of used literature, which includes 91 references.

Main results of the work

1. A comprehensive analysis of the effectiveness of using information theory tools and methods in privacy problems are carried out. The use of differential privacy in Google, IBM libraries, Apple, and the R package are studied. [1, 2]

2. It is proposed to consider normalized mutual information as a measure of image quality assessment, the effectiveness of which is substantiated by experiments and comparison with other quantities. [3]

3. By combining image recognition and privacy protection approaches, a solution to the privacy and verifiability trade-off problem in electronic voting systems is proposed. [4,5]