Katta til modellarining raqamli kriminalistikadagi imkoniyatlari, muammolari va rivojlanish istiqbollari

Bozorov Suhrobjon Mumin o'g'li,
Kriptologiya kafedrasi dotsenti v.b, PhD.
TUIT named after Muhammad al-Khwarizmi,
mr.bozorov95@gmail.com,
ORCID 0000-0002-2377-934X
Yusupova Surayyo Muyasar qizi
suray31052002@gmail.com
doi:https://doi.org/10.5281/zenodo.23034154

Annotatsiya: Ushbu maqolada generativ sun'iy intellekt, xususan katta til modellari (LLM) va raqamli kriminalistikaning kesishuv nuqtasi tizimli tahlil qilinadi. DFRWS (Digital Forensic Research Workshop - Raqamli Kriminalistika Tadqiqotlari Seminari) jarayon modelining oltita bosqichi — identifikatsiya, saqlash, yig'ish, tekshirish, tahlil va taqdim etish — asosida LLM'larning kriminalistik ish jarayoniga integratsiyalashuvining uchta strategik nuqtasi: tekshirish bosqichida ma'lumotlarni aniqlash, tahlil bosqichida dalilni tahlil qilish va taqdim etish bosqichida dalilni hujjatlashtirish batafsil yoritiladi. Maqolada tahdidlarni aniqlash, xotira kriminalistikasi, mobil kriminalistika, bulutli kriminalistika, parol tahlili va bilim grafiklariga asoslangan yondashuvlar kabi ixtisoslashtirilgan yo'nalishlarda erishilgan aniqlik ko'rsatkichlari (85 foizdan 98 foizgacha) keltiriladi. Shu bilan birga, LLM'larning ehtimoliy tabiati bilan kriminalistikaning deterministik talablari o'rtasidagi tub ziddiyat, gallyutsinatsiya (mavjud bo‘lmagan ma’lumotlarni o‘ylab topish) xavfi, kontekst oynasi cheklovlari, standartlashtirilgan baholash metodologiyasining yetishmasligi va huquqiy qabul qilinish muammolari tahlil qilinadi. Xalqaro (Yevropa, Rossiya, AQSh, Xitoy, Yaponiya, Singapur) va milliy (O'zbekiston) kontekstga tayangan holda, sohaning kelajakdagi ilmiy-metodologik yo'nalishlari belgilanadi.

Kalit so'zlar: katta til modellari LLM, raqamli kriminalistika, DFRWS jarayon modeli, generativ sun'iy intellekt, dalil qabul qilinishi, RAG.

Kirish

Raqamli kriminalistika sohasi shaxsiy kompyuterlar va mobil qurilmalarning keng tarqalishidan tortib, bulutli hisoblash va Buyumlar interneti (IoT)ning paydo bo'lishigacha bo'lgan har bir texnologik siljishga javoban uzluksiz rivojlanib kelmoqda, bunda har bir yangi texnologik bosqich raqamli dalilni samarali aniqlash, saqlash, yig'ish, tekshirish va tahlil qilish uchun yangi tahlil metodologiyalari, vositalari va freymvorklarini ishlab chiqishni taqozo etgan [2]. Ushbu sohadagi eng so'nggi tub o'zgarish generativ sun'iy intellektning, xususan ChatGPT, GPT-4, Claude va Gemini kabi katta til modellarining (LLM) jadal rivojlanishi va keng qo'llanilishi bilan bog'liq. Ulkan matnli ma'lumotlar korpusida o'qitilgan ushbu murakkab sun'iy intellekt tizimlari tabiiy tilni tushunish, belgilarni aniqlash va avtomatlashtirilgan mulohaza yuritish borasida raqamli kriminalistik tekshirishlarning asosiy analitik talablariga mos keladigan yuksak qobiliyatlarni namoyon etmoqda [2]. Biroq, LLM'larni raqamli kriminalistika amaliyotiga integratsiyalashuvi ushbu modellar taklif etadigan imkoniyatlar bilan raqamli kriminalistika sohaning qat'iyligi o'rtasida tub ziddiyatlarni keltirib chiqaradi: mavjud raqamli kriminalistik vositalar va metodologiyalar aniq dalillarga ega deterministik tizimlar uchun mo'ljallangan bo'lib, LLM-asosidagi tizimlarning ehtimoliy chiqishi va nodeterministik xatti-harakati bilan to'qnashganda jiddiy qiyinchiliklarga duch keladi [2].

Raqamli kriminalistikaning tub tamoyillari — xususan, takrorlanuvchanlik, dalil zanjirini saqlash va huquqiy qabul qilinish — bir xil kirish ma'lumotlarining bir necha marta chaqirilishida turlicha natija berishi mumkin bo'lgan AI-yordamida olingan imkoniyatlarni qo'shishda ehtiyotkorlik bilan qayta ko'rib chiqilishi lozim. 2022-yil oxirida ChatGPT'ning ommaviy qabul qilinishidan buyon ushbu kesishuv nuqtasida tez sur'atlarda rivojlanayotgan ilmiy adabiyot to'plangan bo'lib, 2023–2025-yillar oralig'ida nashr etilgan ishlarning tizimli tahlili LLM qo'llanilishining joriy manzarasini DFRWS (Digital Forensic Research Workshop - Raqamli Kriminalistika Tadqiqotlari Seminari) jarayon modeli bo'yicha xaritalash imkonini beradi, bunda mavjud imkoniyatlar bilan bir qatorda muhim cheklovlar ham aniqlangan [2; 10]. Ushbu tahlil aniq izchillikni ko'rsatadi: tadqiqot sa'y-harakatlari asosan tekshirish va tahlil bosqichlarida jamlangan bo'lib, bu esa ma'lumotlarni aniqlash va avtomatlashtirilgan mulohaza yuritishdagi LLM imkoniyatlarining dalil yig'ilgandan keyingi faoliyatga tabiiy moslashuvini aks ettiradi. Mazkur maqolaning maqsadi — generativ sun'iy intellekt va raqamli kriminalistikaning kesishuv nuqtasidagi nazariy-arxitekturaviy asoslarni, DFRWS jarayon modeli bo'yicha aniqlangan LLM imkoniyatlarini, hamda ushbu texnologiyalarning amaliy joriy etilishi oldida turgan texnik, uslubiy va institutsional muammolarni tizimli tarzda yoritish, shuningdek sohaning kelgusi ilmiy-tadqiqot yo'nalishlarini belgilashdan iborat. Tadqiqot metodologiyasi tegishli ilmiy adabiyotni tizimli kontent-tahlil qilish, tizimlashtirish va sintez qilish usullariga asoslanadi.

1. Generativ sun'iy intellekt va katta til modellarining nazariy-arxitekturaviy asoslari hamda DFRWS jarayon modeliga integratsiyalashuv nuqtalari

Sun'iy intellekt (AI) tushunchasi odatda inson aqli talab qiladigan vazifalarni — mulohaza yuritish, o'rganish va muammolarni hal qilishni — bajarishga mo'ljallangan hisoblash tizimlarini qamrab oladi; AI'ning kengroq sohasi doirasida mashinaviy o'qitish (ML) — tizimlarga muayyan vazifalar kontekstida ma'lumotlardan naqshlarni o'rganish imkonini beruvchi AI usullari to'plamini, chuqur o'qitish esa ML'ning bir qismi sifatida, ma'lumotlardan ierarxik xususiyatlarni avtomatik ajratib olishga ixtisoslashgan ko'p qatlamli neyron tarmoq arxitekturalarini ifodalaydi [2]. Generativ sun'iy intellekt chuqur o'qitish doirasidagi alohida toifa bo'lib, o'quv ma'lumotlaridan o'rganilgan ma’lumotlar asosida matn, tasvir, audio va kod kabi kontentni generatsiya qila oladigan modellar bilan tavsiflanadi; kirish ma'lumotlari asosida tasniflash yoki taxmin qiluvchi diskriminativ ML modellaridan farqli o'laroq, generativ modellar o'quv ma'lumotlarining asosidagi ehtimollik taqsimotlarini o'rganib, asl korpusga o'xshash yangi namunalarni yaratadi [2]. LLM'lar transformer arxitekturasiga asoslangan generativ AI tizimlarining muhim sinfini tashkil etadi — transformer LLM'lar o'z-o'ziga diqqat (self-attention) mexanizmlari orqali inson tiliga o'xshash matnni qayta ishlaydi va generatsiya qiladi hamda milliardlab tokenlardan iborat ulkan korpuslarda o'qitiladi, bu esa ularga tabiiy tilni tushunish, mulohaza yuritish va vazifalarni umumlashtirish borasida ilgari tabiiy til qayta ishlash yondashuvlaridan farqlanuvchi emergent qobiliyatlarni namoyon etish imkonini beradi [2].

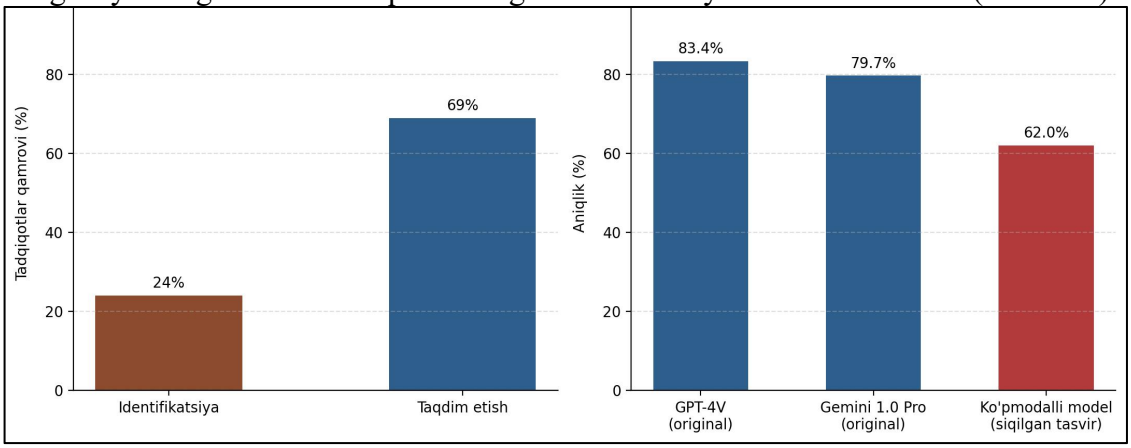
Transformer arxitekturasining o'zagini tashkil etuvchi o'z-o'ziga diqqat mexanizmi butun matn ketma-ketligini parallel qayta ishlash imkonini berib, modelga murakkab bayonlarni tushunish uchun zarur bo'lgan uzoq masofali bog'liqliklar va kontekstual munosabatlarni qamrab olish qobiliyatini beradi [2; 5]. Ushbu arxitekturaviy asos raqamli kriminalistik qo'llanilishlarga bevosita tegishli bo'lgan bir qator qobiliyatlarni qo'llab-quvvatlaydi: kontekstual tushunish modellarga noaniq havolalarni talqin qilish, so‘zlarni hal qilish va uzaytirilgan suhbat almashinuvlari davomida izchillikni saqlash imkonini beradi, bu esa aloqa jurnallarini tahlil qilish va parchalangan dalillardan voqealar ketma-ketligini tiklashda qimmatli bo'ladi; ma'lumotlarni aniqlash qobiliyatlari LLM'larga aniq qoidaga asoslangan dasturlashsiz g'ayrioddiy xatti-harakatlar va hujum imzolarini aniqlash hamda turli dalil manbalarini o'zaro bog'lash imkonini beradi; semantik mulohaza yuritish esa modellarga

ob'ektlar o'rtasidagi bilvosita munosabatlarni xulosa qilish va sabab-oqibat aloqalari haqida gipotezalar shakllantirish imkonini beradi [2].

Shu bilan birga, ushbu qobiliyatlar raqamli kriminalistik qo'llanilishlarga bevosita ta'sir qiluvchi tabiiy cheklovlar bilan birga keladi: harorat (temperature) kabi parametrlar tomonidan boshqariladigan LLM chiqishini generatsiya qilishning ehtimoliy tabiati nodeterministiklikni keltirib chiqaradi, bunda bir xil kirish ma'lumotlari bir necha marta chaqirilganda turlicha chiqish natijasini berishi mumkin, bu esa raqamli dalilning takrorlanuvchanlik talablariga va huquqiy qabul qilinishiga tub jihatdan zid keladi; bundan tashqari, LLM'lar gallyutsinatsiyaga kuchli moyillikni namoyon etadi, ya'ni tekshirilmasa tahlilni adashtirishi mumkin bo'lgan, ishonarli, ammo faktik jihatdan noto'g'ri ma'lumotni generatsiya qiladi [11]; nihoyat, transformer arxitekturalariga xos kontekst oynasi cheklovlari bir vaqtning o'zida qayta ishlanishi mumkin bo'lgan ma'lumot hajmini cheklaydi, bu esa yirik ko'lamli kriminalistik ma'lumotlar to'plamlarining tahlilini parchalab yuborishi mumkin [2].

Ushbu nazariy-texnik asosga tayangan holda, LLM imkoniyatlarini o'rnatilgan tekshiruv jarayonlariga tizimli tarzda joylashtirish uchun DFRWS jarayon modeli asos sifatida qo'llaniladi, u oltita asosiy bosqichni o'z ichiga oladi: identifikatsiya bosqichi turli elektron qurilmalar va tizimlar bo'ylab raqamli dalil manbalarini aniqlashni; saqlash bosqichi kriptografik xeshlash va tegishli saqlash mexanizmlari orqali aniqlangan dalilning yaxlitligini ta'minlashni; yig'ish bosqichi yozishdan himoyalangan qurilmalar va tasdiqlangan kriminalistik vositalar yordamida bit-bit nusxalarni yaratishni; tekshirish bosqichi shifrlashni chetlab o'tish, o'chirilgan fayllarni tiklash va katta hajmdagi ma'lumotlarni qayta ishlashni talab qiluvchi ma'lumotlarni sistematik baholash va tegishli axborotni ajratib olishni; tahlil bosqichi bir necha manbalar bo'ylab dalilni bog'lash, gipotezalarni ishlab chiqish va sinash hamda raqamli artefaktlar bilan tekshiruv savollari o'rtasida sabab-oqibat munosabatlarini o'rnatishni; nihoyat, taqdim etish bosqichi topilmalarni hujjatlashtirish va ekspert xulosaligini berishni o'z ichiga oladi [2; 6].

Ushbu model asosida o'tkazilgan tizimli tahlil LLM imkoniyatlari kriminalistik talablarga mos keladigan uchta strategik integratsiya nuqtasini aniqladi — tekshirish bosqichida ma'lumotlarni aniqlash, tahlil bosqichida dalilni tahlil qilish va taqdim etish bosqichida dalilni taqdim etish va hisobot berish — bunda tadqiqot ishlarining aksariyati aynan tekshirish va tahlil bosqichlarida jamlangan, identifikatsiya bosqichi esa faqat ishlarning 24 foizida, asosan yaxlit uchdan-uchgacha freymvorklarni taklif qiluvchi ishlarda yoritilgan, taqdim etish bosqichi esa ishlarning 69 foizida, avtomatlashtirilgan hisobot yaratish va dalilni yetkazish qobiliyatlariga alohida e'tibor bilan qamrab olingan, saqlash va yig'ish bosqichlari esa deyarli e'tiborsiz qolgan, bu holat ixtisoslashtirilgan apparat va dasturiy vositalarga tayanadigan ushbu bosqichlarning texnik xususiyati bilan izohlanadi (1-2-rasm).



1- 2-rasm. DFRWS jarayon modeli bosqichlari bo'yicha tadqiqotlar qamrovi hamda ko'pmodelli tahlil aniqligining siqilgan tasvirlarda pasayishi [2].

2. LLM'larning kriminalistik ish jarayonining turli bosqichlarida qo'llanilishi: aniqlangan imkoniyatlar va empirik natijalar

Ma'lumotlarni aniqlash tekshirish bosqichidagi muhim integratsiya nuqtasi bo'lib, bunda LLM'lar tekshiruv olib boruvchilarga ma'lumot manbalari bo'ylab kriminalistik artefaktlarni aniqlash, g'ayrioddiy xatti-harakatlarni aniqlash va hujum imzolarini tanib olishda yordam beradi. Umumiy maqsadli modellar Windows hodisa jurnallari, reestr qiymatlari va prefetch fayllari kabi operatsion tizim artefaktlarini, shuningdek Google Drive kabi bulutli platformaga xos artefaktlarni aniqlashda samaradorlik ko'rsatgan, garchi yo'l aniqlashda vaqti-vaqti bilan noaniqliklar kuzatilgan bo'lsa-da [2]. Nol-namunali o'qitish (zero-shot learning) yondashuvlari yordamida kriminalistik vaqt chiziqlaridagi anomaliyalarni aniqlash uchun beshta ochiq ma'lumotlar to'plami bo'yicha oldindan o'qitilgan olti xil model baholanganda, salbiy sentiment tasnifini shubhali hodisa ko'rsatkichi sifatida ko'rib chiqish orqali domenga xos o'qitishsiz g'ayrioddiy jurnal yozuvlarini aniqlash mumkinligi isbotlangan, biroq modellar orasidagi sezilarli samaradorlik farqi (21,8 foizgacha) model tanlovining o'zi tanqidiy kriminalistik qaror ekanligini ko'rsatgan [2]. Kiber hodisa vaqt chizig'ini tahlil qilishga Retrieval-Augmented Generation (RAG) texnologiyasini Llama 3.1 8B modeli bilan integratsiyalashgan semantik boyitish freymvorki qo'llanilganda, olti xil hodisa ssenariysi (SYN-flood hujumi, fishing, DNS-spoofing) bo'yicha dalil qidirib topishda 100 foizlik aniq moslik ko'rsatkichiga va umumiy 97,51 foizlik samaradorlikka erishilgan, bu esa diqqat mexanizmiga asoslangan yondashuvning har bir hodisaning tekshiruv so'roviga nisbatan ahamiyatini og'irlashtirish orqali oddiy vaqtinchalik korrelyatsiyadan ustunligini ko'rsatadi [2; 3].

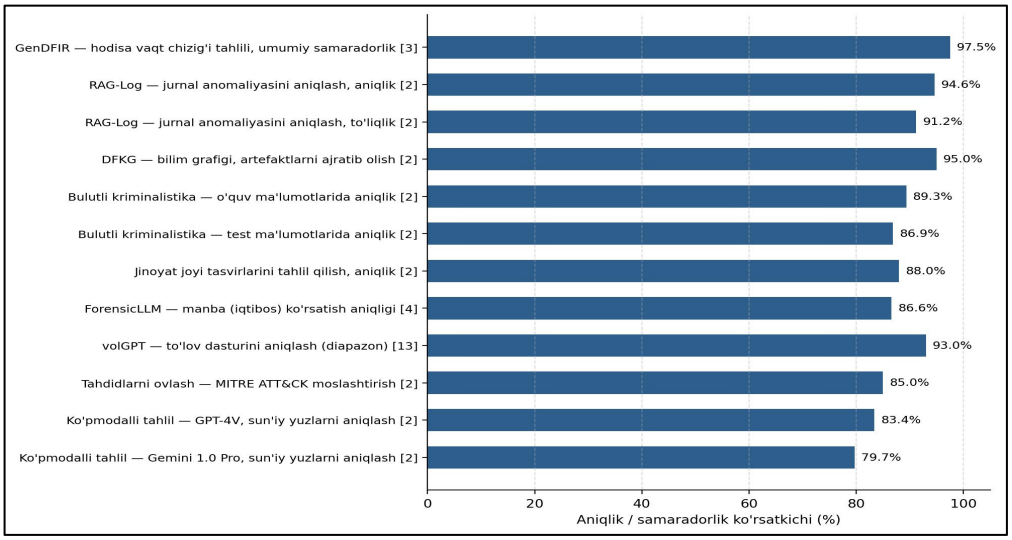
Muntazam ifodalar va kalit so'zlar ro'yxatini generatsiya qilish borasida umumiy maqsadli modellar kredit karta raqamlari va avtomobil davlat raqami belgilari kabi keng tarqalgan ob'ektlar uchun batafsil ma’lumotlarni tushuntirishlar bilan birga taqdim eta olgan, biroq generatsiya qilingan ifodalar bo'shliqlarni hisobga olmaslik kabi cheklovlarga ega bo'lib, ularni amaliyotga joriy etishdan oldin sinovdan o'tkazish zarurligini ko'rsatgan [2]. Jurnal anomaliyalarini avtomatik aniqlash uchun RAG texnologiyasini GPT-3.5 bilan integratsiyalashgan freymvork shubhali jurnal yozuvlarini aniqlashda 94,6 foizlik aniqlik va 91,2 foizlik to'liqlikka erishgan, shu bilan birga 100 ming jurnal yozuvidan iborat ma'lumotlar to'plami uchun tahlil vaqtini o'rtacha 4,2 soatdan atigi 18 daqiqagacha qisqartirgan, biroq bu yondashuv yuqori sifatli o'quv ma'lumotlariga jiddiy bog'liqlik ta'siriga zaiflikni saqlab qolgan [2]. Tahdidlarni aniqlash avtomatlashtirilishi borasida Code Llama va LLaMA 3 asosidagi freymvork turli hujum naqshlari bo'ylab 85 foizdan yuqori aniqlash darajasiga erishgan, bunda kuzatilgan tahdid ko'rsatkichlarini MITRE ATT&CK freymvorkiga tizimli tarzda moslashtirish orqali an'anaviy ravishda keng qamrovli qo'lda tahlilni talab qiladigan murakkab ma'lumotlarni aniqlash vazifalarini avtomatlashtirish qobiliyati namoyon etilgan [2].

Dalilni tahlil qilish bosqichida LLM'lar tabiiy tildagi tekshiruv savollarini tuzilgan so'rovlarga tarjima qilish qobiliyatini namoyon etgan — masalan, Hansken kriminalistik platformasi uchun Hansken So'rov Tilida (HQL) sintaktik jihatdan to'g'ri so'rovlarni generatsiya qilish orqali, muayyan sana oralig'ida biriktirmali elektron xatlarni aniqlash yoki muayyan foydalanuvchilar tomonidan fayl bajarilishi dalilini topish kabi keng tarqalgan kriminalistik ssenariylarni qamrab olgan holda [2]. Kod tahlili va generatsiyasi borasida LLM'lar fayl tiklash (file carving) operatsiyalari uchun yaxshi izohlangan Python kodini, shu jumladan sarlavhadan yakungacha bo'lgan ajratib olish naqshlarini generatsiya qilishga qodir bo'lgan, RAID massivlarini olish ssenariylarida esa RAID darajasini aniqlash va disk tasvirlarini yaratish funksiyalarini generatsiya qilgan, biroq generatsiya qilingan skriptlar bir necha disklar bo'ylab RAID izchilligini tekshirish mexanizmlaridan mahrum bo'lgan [2]. Ko'pmodelli dalilni tahlil qilishda GPT-4V va Gemini 1.0 Pro sun'iy generatsiya qilingan yuz tasvirlarini aniqlashda mos ravishda 83,4 foiz va 79,7 foizlik aniqlikka erishgan, biroq

siqilgan tasvirlar tahlil qilinganda samaradorlik taxminan 62 foizgacha pasaygan; jinoyat sodir bo'lgan joy tasvirlarini tahlil qilishda esa ko'pmodelli dalil ob'ektlarini aniqlash va fazoviy munosabatlarni tahlil qilishda ekspert insoniy tahlil bilan taqqoslaganda 88 foizlik aniqlikka erishib, tahlil vaqtini 43 foizga qisqartirgan [2].

Ixtisoslashtirilgan kriminalistik yo'nalishlarda ham sezilarli natijalarga erishilgan: kontekstga asoslangan parol lug'atlarini generatsiya qiluvchi freymvork oddiy lug'at hujumlariga nisbatan qiyin deb baholangan parollar uchun 50 foizgacha samaradorlik oshishini ta'minlagan [12]; xotira kriminalistikasida GPT-3.5-turbo'ni Volatility vositasi bilan integratsiyalashgan freymvork beshta to'lov dasturi oilasi bo'yicha 87 dan 99 foizgacha aniqlik ko'rsatgan holda qo'lda tekshiruv talab qiluvchi shubhali jarayonlar sonini taxminan 90 foizga qisqartirgan [13], Volatility 3, YARA imzoga asoslangan aniqlash va Mistral-7B xulosalashni birlashtirgan yana bir integratsiyalashgan vosita esa LLM komponentini olib tashlash F1-ko'rsatkichni 10 foizgacha pasaytirishini ko'rsatib, uning qo'shgan hissasini tasdiqlagan; mobil kriminalistikada ko'pmodelli LLM va optik belgi tanish (OCR) texnologiyasini birlashtirgan freymvork jismoniy Android qurilmalarini real vaqtda tahlil qilishga, tabiiy til tavsiflari orqali foydalanuvchi harakatlarini simulyatsiya qilishga imkon bergan; bulutli kriminalistikada oz-namunali o'qitishga asoslangan freymvork Random Forest, XGBoost va Gradient Boosting kabi an'anaviy mashinaviy o'qitish modellariga nisbatan yuqoriroq aniqlik (o'quv ma'lumotlarida 89,34 foiz, test ma'lumotlarida 86,87 foiz) ko'rsatgan; bilim grafigiga asoslangan yondashuvlar orasida IoT kriminalistikasi uchun BERT va RoBERTa modellarini grafik neyron tarmoqlari bilan birlashtirgan tizim 6 milliondan ortiq noyob ob'ekt va 45 million uch birlikni qayta ishlagan, 13 GB hajmidagi, 61 ta ilova, 2864 ta ma'lumotlar bazasi va 5870 ta jadvalni o'z ichiga olgan kriminalistik tasvir asosida ishlaydigan boshqa bir freymvork esa artefaktlarni ajratib olishda 95 foizdan yuqori aniqlikka va to'liq dalil zanjirini saqlashga erishgan, GPT-4o modeli esa mobil qurilma ma'lumotlaridan dalillar tarmog'ini avtomatik quruvchi 'Forensic Intelligence Graphs' yaratish uchun qo'llanilgan [2; 4].

Chinakam huquqni muhofaza qilish kontekstida, Koreya Milliy politsiya agentligining jinoyat tergovlaridan olingan 140 mingdan ortiq haqiqiy kriminalistik xabarlar asosida GPT-4o, Gemini 1.5 va Claude 3.5 modellarining aniqlik, to'liqlik, F1-ko'rsatkich va gallyutsinatsiya darajasi bo'yicha qiyosiy tahlili o'tkazilgan, bunda GPT-4o eng yuqori umumiy samaradorlikka erishgan [2; 14]. Dalilni taqdim etish bosqichida, tekshiruv nazariyalari va ilmiy adabiyot asosida o'qitilgan hamda Retrieval Augmented Fine-tuning (RAFT) metodologiyasi orqali maxsus sozlangan ixtisoslashtirilgan model manbani 86,6 foiz hollarda to'g'ri ko'rsatgan holda, tekshiriluvga asoslangan kriminalistik tushuntirishlarni generatsiya qilish qobiliyatini namoyon etgan, bu esa uni maxfiy ish ma'lumotlarini uchinchi tomon bulutli xizmatlariga oshkor qilmasdan qayta ishlash imkonini beruvchi maxfiylikni saqlovchi mahalliy joylashtirish arxitekturasi bilan birlashtirgan holda taqdim etadi [2; 4]. Strukturaviy dalil taqdimoti borasida esa deterministik noyob identifikatorlar (UID) orqali dalil zanjiriga rioya qilishni saqlagan holda, Raqamli Kriminalistik Bilim Grafigi (DFKG) generatsiya qilish artefaktlarni ajratib olishda 95 foizdan yuqori aniqlikka erishgan [2].



3-rasm. LLM asosidagi turli kriminalistik tizimlarning erishgan aniqlik va samaradorlik ko'rsatkichlari[2; 3; 4; 13].

3. LLM-yordamidagi raqamli kriminalistikaning texnik, uslubiy va institutsional muammolari hamda kelgusi rivojlanish yo'nalishlari

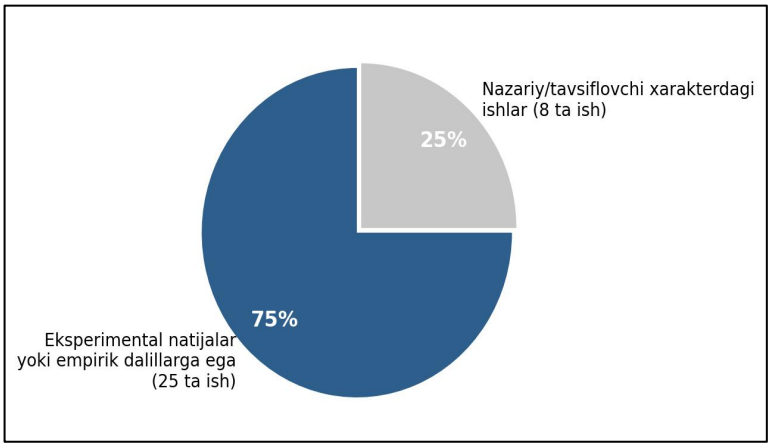
LLM'larni raqamli kriminalistik ish jarayoniga integratsiyalashuvi ijobiy tomonlar bilan bir qatorda ko'p qirrali muammolar to'plamini ham keltirib chiqaradi, bu muammolar odatda yettita kontseptual jihatdan farqlanuvchi toifaga ajratiladi: texnik muammolar model dizaynining asosiy cheklovlari va hisoblash talablariga tegishli; uslubiy muammolar LLM imkoniyatlarini qanday baholash va kriminalistik ish jarayoniga qanday integratsiyalash masalalariga qaratilgan; kriminalistik yaxlitlik muammolari ilmiy qat'iylik va dalilga oid standartlarga javob berishga qaratilgan; ma'lumotlar boshqaruvi va xavfsizligi maxfiylik, konfidensiallik va joylashtirish xavfsizligi masalalarini qamrab oladi; operatsion joriy etish muammolari real kriminalistik sharoitlarda amaliy joriy etish to'siqlariga tegishli; domenga xos cheklovlar muayyan kriminalistik vazifalar va raqamli dalil turlaridan kelib chiqadigan cheklovlarni o'zida mujassam etadi; nihoyat, tizimlilik va adolatlilik muammolari o'quv ma'lumotlaridagi algoritmik qarorlarning turli populyatsiyalar bo'ylab notekis natijalarga olib kelishi mumkinligini o'rganadi [2]. Texnik jihatdan, LLM chiqishini generatsiya qilishning ehtimoliy tabiati takrorlanuvchanlikni talab qiluvchi raqamli kriminalistik qo'llanilishlar uchun tub muammolarni keltirib chiqaradi — bir xil kirish ma'lumotlari, xususan tarmoq paketlarini talqin qilishda, bir necha so'rovda turlicha va noto'g'ri natijalar berishi mumkinligi isbotlangan, bu esa nazorat ostidagi sharoitlarda bir xil kirish ma'lumotlariga qo'llanilganda izchil natija berishi shart bo'lgan kriminalistik metodlarning qat'iy takrorlanuvchanlik talablariga tubdan zid keladi, bunda hatto yuqori aniqlik ko'rsatkichlariga (95 foizdan yuqori) erishilgan holatlarda ham ehtimoliy generatsiya mexanizmi deterministik validatsiya nazorati va keng qamrovli audit izlari orqali ehtiyotkorlik bilan boshqarilishi lozim bo'lgan o'zgaruvchanlikni keltirib chiqaradi [2].

Kontekst oynasi cheklovlari bir vaqtning o'zida qayta ishlanishi mumkin bo'lgan ma'lumot hajmini tub jihatdan cheklaydi, zamonaviy modellar o'quv kontekst uzunligidan oshgan kirish ketma-ketliklarini qayta ishlashda U-shaklidagi samaradorlik egri chizig'ini namoyon etadi, bunda uzun kontekstning boshi va oxiridagi ma'lumot o'rtasidagi mazmunga nisbatan samaraliroq qayta ishlanadi, bu esa model sig'imi cheklovlaridan oshib ketadigan yirik ko'lamli kriminalistik ma'lumotlar to'plamlarini tahlil qilishda jiddiy muammolarni keltirib chiqaradi va tekshiruvchilardan mazmunli bog'liqliklarni parchalab yuborishi mumkin bo'lgan bo'laklarga bo'lish strategiyalarini joriy etishni talab qiladi [2]. Gallyutsinatsiya — LLM'lar tekshirilmasa tergovni adashtirishi mumkin bo'lgan ishonarli, ammo faktik jihatdan noto'g'ri ma'lumotni generatsiya qilganda yuzaga keladigan — muhim texnik cheklov bo'lib,

mavjud bo'lmagan vosita nomlari va haqiqatda mavjud bo'lmagan manbalarni yuqori ishonch bilan generatsiya qilish holatlari hujjatlashtirilgan, bu muammo gallyutsinatsiyalangan kontentni tashqi tekshiruvsiz qonuniy ma'lumotdan ajratishning qiyinligi bilan yanada murakkablashadi, bu esa har qanday chiqarilgan dalilning har doim inson tomonidan tekshirilishini talab qiladi [2]. Uslubiy nuqtai nazardan, LLM-yordamidagi kriminalistik vazifalar uchun standartlashtirilgan baholash freymvorklarining yo'qligi tadqiqotlar o'rtasida mazmunli taqqoslashga to'sqinlik qiladi va kumulyativ bilim rivojlanishini cheklaydi, turli tadqiqotlar bir-biriga mos kelmaydigan metrikalar, baholash mezonlari va eksperimental dizaynlarga tayanadi, bu esa muqobil yondashuvlarni tizimli taqqoslashni imkonsiz qiladi; standartlashtirish borasidagi so'nggi harakatlar va'dali bo'lsa-da, ular hali cheklangan doirada qolmoqda va nazorat ostidagi muhitlar hamda sintetik ma'lumotlarga ega alohida tadqiqotlar bilan cheklangan [2].

Adabiyotda sintetik ma'lumotlar to'plamiga ustuvor tayanish eksperimental validatsiya bilan isbotlangan operatsion qo'llanilish o'rtasida sezilarli bo'shliqni keltirib chiqaradi — hatto sintetik kiber hodisa voqealarida 97,51 foizlik umumiy samaradorlikka erishilgan holatlarda ham, bu natijalarning real, murakkab va ko'p tomonlama tekshiruv sharoitlariga to'g'ridan-to'g'ri o'tkazilishi hali alohida tekshiruvni talab qiladi [2]. Ushbu texnik va uslubiy cheklovlardan tashqari, kriminalistik yaxlitlik, ma'lumotlar boshqaruvi, operatsion joylashtirish toifalari ham o'zaro bog'liq muammolarni keltirib chiqaradi: xususan, bulutli LLM xizmatlaridan foydalanish nozik ish ma'lumotlarining uchinchi tomonlarga oshkor bo'lish xavfini tug'dirsa, mahalliy joylashtirish ma'lumotlar suvereniteti muammosini ma'lum darajada yechadi-yu, ammo hisoblash resurslariga bo'lgan talabni oshiradi. Kelgusi tadqiqot yo'nalishlari texnik, uslubiy va huquqiy sohalarni qamrab oluvchi keng qamrovli kun tartibini belgilaydi, bunda kriminalistikaga tayyor LLM arxitekturalarini, standartlashtirilgan validatsiya freymvorklarini va inson-AI hamkorlik yondashuvlarini ishlab chiqish alohida ustuvor yo'nalishlar sifatida ajratib ko'rsatiladi; jumladan, ontologiyaga asoslangan bilim ifodasi va Javob To'plami Dasturlashtirish (ASP) validatsiya qoidalarini ko'pmodelli LLM'lar bilan birlashtirgan neyro-simvolik yondashuvlar LLM tomonidan generatsiya qilingan xulosalarni rasmiy mantiqiy qoidalar to'plamiga nisbatan tekshiruvchi aniq mulohaza yuritish mexanizmlarini integratsiyalash orqali kriminalistik talablarni qondirishga qaratilgan bo'lib, bunday yondashuv kriminalistik xulosalar uchun xulq-atvorning rasmiy kafolatlarini va inson tomonidan izohlanadigan tushuntirishlarni ta'minlashi, shu orqali sud-ekspertiza xizmati ko'rsatuvchilar uchun ISO 17025 akkreditatsiya standartlariga muvofiqlashishi mumkinligini ko'rsatadi [2].

Bunday interfaol-tekshiriluvchi yondashuvlarga bo'lgan ehtiyoj global miqyosda tan olinmoqda — xususan, chuqur o'qitishga asoslangan kiberxavfsizlik yechimlarini ko'p mezonli va qat'iy tarzda baholash zarurligi Rossiya ilmiy adabiyotida ham alohida ta'kidlangan [7], AQSh Milliy standartlar va texnologiyalar instituti tomonidan ishlab chiqilgan kriminalistik jarayon uslubiy asosi esa har qanday yangi texnologiyaning, jumladan LLM'larning, integratsiyalashuvi tekshirish, tahlil va hisobot berish bosqichlarining ilmiy asoslanganligini saqlashi zarurligini ko'rsatadi [8], Osiyo mintaqasida esa LLM'larni raqamli tergovga integratsiyalashuvi mintaqalararo tadqiqot yo'nalishi sifatida, ehtiyotkor baholash freymvorklarini talab qiluvchi masala sifatida ko'rib chiqilmoqda [9]. O'zbekiston kontekstida, 'Kiberxavfsizlik to'g'risida'gi Qonunga muvofiq belgilangan institutsional-huquqiy asos [1] LLM-yordamidagi kriminalistik vositalarning kelgusida milliy amaliyotga joriy etilishi uchun tayanch nuqta bo'lib xizmat qilishi mumkin, biroq bunday integratsiya, xalqaro tajriba ko'rsatganidek, faqat qat'iy validatsiya, inson nazorati va sohaga xos me'yoriy-uslubiy asoslar mavjud bo'lgandagina kriminalistik yaxlitlikni saqlagan holda amalga oshirilishi mumkin.



4-rasm. Eksperimental natijalarga ega bo'lish nisbati. [2].

Xulosa

O'tkazilgan tahlil generativ sun'iy intellekt, xususan katta til modellarining raqamli kriminalistika sohasiga integratsiyalashuvi ikki tomonlama xarakterga ega ekanligini ko'rsatdi. Bir tomondan, LLM'lar DFRWS jarayon modelining tekshirish, tahlil va taqdim etish bosqichlarida, ma'lumotlarni aniqlashdan tortib xotira kriminalistikasi, mobil kriminalistika, bulutli kriminalistika va bilim grafiklariga asoslangan dalil tarmoqlarini qurishgacha bo'lgan xilma-xil vazifalarda 85 foizdan 98 foizgacha aniqlikka erishib, sezilarli samaradorlik yutuqlarini namoyon etdi, bu esa an'anaviy qo'lda bajariladigan tahlil jarayonlarini sezilarli darajada tezlashtirish salohiyatiga ega. Ikkinchi tomondan, LLM chiqishining ehtimoliy tabiati bilan raqamli kriminalistikaning deterministik, takrorlanuvchan va huquqiy jihatdan qabul qilinadigan natijalarga bo'lgan talabi o'rtasidagi tub ziddiyat, gallyutsinatsiya xavfi, kontekst oynasi cheklovlari va standartlashtirilgan baholash metodologiyasining yetishmasligi kabi jiddiy muammolar ushbu texnologiyalarning operatsion muhitlarga to'liq joriy etilishini cheklab turibdi. Shu sababli, hozirgi bosqichda LLM'lar mustaqil kriminalistik dalil manbai emas, balki inson tomonidan majburiy tekshirilishi lozim bo'lgan yordamchi vosita sifatida qaralishi zarur. Kelgusi tadqiqotlar kriminalistikaga tayyor LLM arxitekturalarini, standartlashtirilgan validatsiya protokollarini va neyro-simvolik tekshiruv mexanizmlarini ishlab chiqishga, shuningdek texnik, uslubiy va huquqiy sohalar o'rtasidagi fanlararo hamkorlikni mustahkamlashga qaratilishi lozim, bu esa nafaqat xalqaro, balki O'zbekiston milliy kriminalistik tizimlar uchun ham ushbu texnologiyalarni ishonchli va qonuniy tarzda joriy etishning zaruriy shartidir.

Foydalanilgan adabiyotlar

1. **I. Qonunchilik hujjatlari**
2. [1] O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni, O'RQ-764-son, 2022-yil 15-aprel (2022-yil 17-iyuldan kuchga kirgan). Manba: O'zbekiston Respublikasi qonun hujjatlari milliy ma'lumotlar bazasi — lex.uz. Havola: https://lex.uz/uz/docs/-5960604
3. **II. Ilmiy maqolalar**
4. [2] Chernyshev M., Baig Z., Syed N., Doss R., Shore M. Large language models in digital forensics: capabilities, challenges and future directions // Forensic Science International: Digital Investigation. — 2026. — Vol. 56, Art. 302043. DOI: 10.1016/j.fsidi.2025.302043. URL: https://www.sciencedirect.com/science/article/pii/S2666281725001830
5. [3] Loumachi F.Y., Ghanem M.C., Ferrag M.A. Advancing Cyber Incident Timeline Analysis Through Retrieval-Augmented Generation and Large Language Models //

Computers (MDPI). — 2025. — Vol. 14, No. 2, Art. 67. DOI: 10.3390/computers14020067.
6. [4] Sharma B., Ghawaly J., McCleary K., Webb A.M., Baggili I. ForensicLLM: A local large language model for digital forensics // Forensic Science International: Digital Investigation. — 2025. — Vol. 52, Art. 301872. DOI: 10.1016/j.fsidi.2025.301872.
7. [5] Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A.N., Kaiser Ł., Polosukhin I. Attention Is All You Need // Advances in Neural Information Processing Systems (NeurIPS). — 2017. — Vol. 30. arXiv:1706.03762.
8. [6] Palmer G. A Road Map for Digital Forensic Research // Report from the First Digital Forensic Research Workshop (DFRWS), Technical Report DTR-T001-01. — 2001.
9. [7] Использование больших языковых моделей для поиска угроз кибербезопасности на основе методов глубокого обучения: анализ современных исследований // КиберЛенинка (электронная научная библиотека). URL: https://cyberleninka.ru/article/n/ispolzovanie-bolshih-yazykovyh-modeley-dlya-poiska-ugroz-kiberbezopasnosti-na-osnove-metodov-glubokogo-obucheniya-analiz
10. [8] Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response // NIST Special Publication 800-86. — Gaithersburg: National Institute of Standards and Technology, 2006. — 121 p. URL: https://csrc.nist.gov/pubs/sp/800/86/final
11. [9] Chaudhary N.K., Iyengar S.S., Saidakhrarovich G.S. Large Language Models for Digital Forensic Investigations // Information Security, Privacy and Digital Forensics. ICISPD 2024. Lecture Notes in Electrical Engineering, vol. 1456. — Singapore: Springer, 2026. DOI: 10.1007/978-981-95-2196-8_18
12. [10] Wickramasekara A., Breitinger F., Scanlon M. Exploring the Potential of Large Language Models for Improving Digital Forensic Investigation Efficiency // Forensic Science International: Digital Investigation. — 2025. — Vol. 52, Art. 301859.
13. [11] Scanlon M., Breitinger F., Hargreaves C., Hilgert J.-N., Sheppard J. ChatGPT for digital forensic investigation: the good, the bad, and the unknown // Forensic Science International: Digital Investigation. — 2023. — Vol. 46, Art. 301609.
14. [12] Rando J., Hitaj D., et al. PassGPT: Password Modeling and (Guided) Generation with Large Language Models // Computer Security – ESORICS 2023, Lecture Notes in Computer Science, vol. 14345. — Cham: Springer, 2024. arXiv:2306.01545.
15. [13] Oh D.B., et al., Kim H.K. volGPT: Evaluation on triaging ransomware process in memory forensics with Large Language Model // Forensic Science International: Digital Investigation. — 2024. — Vol. 49, Supplement, Art. 301756.
16. [14] Kim K.-J., et al., Kang W. Digital forensics in law enforcement: A case study of LLM-driven evidence analysis // Forensic Science International: Digital Investigation. — 2025. — Vol. 54, Art. 301939.
17. **III. Ilmiy tezislar va dissertatsiyalar**
18. [15] Sharma B. ForensicLLM: A Local Large Language Model for Digital Forensics // LSU Master's Theses, No. 6059. — Louisiana State University, 2024. URL: https://repository.lsu.edu/gradschool_theses/6059/
19. **IV. Veb-manbalar**
20. [16] NPO Institute of Digital Forensics (IDF), founded 2004, Japan — Organization overview. URL: https://digitalforensic.jp/home/idf/
21. [17] Frontier Applications of Artificial Intelligence in Digital Forensics // CSDN Blog. — 2025-04-12. URL: https://blog.csdn.net/weixin_30798867/article/details/147190439