

**O‘ZBEKISTON RESPUBLIKASI ADLIYA VAZIRLIGI
X.SULAYMONOVA NOMIDAGI RESPUBLIKA SUD EKSPERTIZASI
MARKAZI**



**VIDEO VA FOTO TASVIRLARNING
HAQIQIYLIGINI ANIQLASHDA E'TIBOR
QILINADIGAN JIHATLAR**

(Fuqarolar uchun qo'llanma)

Toshkent 2026

Mualliflar jamoasi: X. Sulaymonova nomidagi Respublika sud ekspertiza markazi Sud-kompyuter texnikaviy ekspertizasi bo‘limi boshlig‘i D.Sh. Ataniyazov, bo‘lim yetakchi eksperti J.Z. Abdukarimov, bo‘lim eksperti D.R.Eshpo‘latov

Ushbu qo‘llanma video va foto tasvirlarning haqiqiyligini aniqlashda e‘tibor qilinadigan jihatlarbo‘yicha fuqarolar tomonidan foydalanish uchun tayyorlangan.

© X. Sulaymonova nomidagi RSEM 2026 y.

KIRISH

Hozirgi kunda internet va ijtimoiy tarmoqlarning rivojlanishi natijasida video hamda foto tasvirlar kundalik hayotimizning ajralmas qismiga aylandi. Turli platformalarda har kuni millionlab surat va videolar tarqatiladi. Biroq barcha tarqatilayotgan materiallar ham haqiqiy va ishonchli bo'la olmaydi. Zamonaviy dasturlar yordamida tasvirlarni o'zgartirish, montaj qilish, sun'iy intellekt orqali yangi tasvir yaratish yoki mavjud videolarni soxtalashtirish imkoniyati kengayib bormoqda. Soxta yoki manipulyatsiya qilingan foto va videolar fuqarolarni chalg'itishi, noto'g'ri ma'lumot tarqalishiga sabab bo'lishi, shaxs sha'ni va qadr-qimmatiga zarar yetkazishi, firibgarlik holatlariga olib kelishi mumkin. Shu sababli har bir fuqaro video va foto tasvirlarning haqiqiylikni aniqlash bo'yicha asosiy bilimlarga ega bo'lishi muhim hisoblanadi.

Mazkur qo'llanmada video va foto tasvirlarning haqiqiylikni aniqlashda e'tibor qaratilishi kerak bo'lgan jihatlar, amaliy tekshiruv usullari hamda xavfsizlik tavsiyalari bayon etiladi.

Foto va video tasvirlarning haqiqiyliги nima?

Foto yoki video tasvirning haqiqiyliги — undagi ma'lumotlar asl holatda saqlanganliги, tasvir sun'iy ravishda o'zgartirilmaganliги va voqelikni to'g'ri aks ettirishini anglatadi.

Tasvirlarga quyidagi usullar orqali o'zgartirish kiritilishi mumkin:

- foto montaj qilish;
- videoni kesish va birlashtirish;
- tasvirga qo'shimcha obyektlar kiritish;
- ovozni almashtirish;
- sun'iy intellekt (AI) yordamida yuz yoki ovoz yaratish;
- rang va yorug'likni sun'iy o'zgartirish;
- metadata ma'lumotlarini tahrirlash.

Bunday o'zgartirishlar ayrim hollarda oddiy ko'rinishi mumkin, biroq noto'g'ri maqsadlarda foydalanilganda jiddiy oqibatlariga olib keladi.

!Eslatma

UNESKO ma'lumotlariga ko'ra, ijtimoiy tarmoqlarda yolg'on ma'lumotlar haqiqiy yangilikga nisbatan 6 barobar tezroq tarqaladi.

Fotosuratlarini tekshirish

Fotosuratlar soxtalashtirilganda ko'pincha detallarda xatoliklarga yo'l qo'yiladi.

1. Tasvir sifati va piksel tahlili

Raqamli foto va video tasvirlarning haqiqiylikni aniqlashda eng muhim usullardan biri tasvir sifati hamda piksel tahlili hisoblanadi. Har qanday raqamli tasvir millionlab piksellardan tashkil topgan bo'lib, ular rang, yorug'lik va tasvir

tafsilotlarini ifodalaydi. Agar tasvirga tashqi aralashuv amalga oshirilsa, masalan obyekt qo'shilsa, o'chirib tashlansa yoki fon almashtirilsa, bu holat piksel tuzilishida ma'lum izlar qoldiradi. Shu sababli kriminalistika va raqamli ekspertiza sohasida piksel tahlili eng asosiy tekshiruv metodlaridan biri hisoblanadi. Tasvir montaj qilinganda ko'pincha tasvirning ayrim qismlarida sifat farqi paydo bo'ladi. Masalan, original kamera orqali olingan suratning barcha qismlarida siqilish darajasi bir xil bo'ladi. Agar keyinchalik boshqa obyekt qo'shilgan bo'lsa, o'sha obyektning aniqligi, rang chuqurligi yoki kontrasti boshqa qismlardan farq qilishi mumkin. Buni oddiy ko'z bilan aniqlash qiyin bo'lsa-da, maxsus ekspertiza dasturlari orqali aniqlash mumkin. Piksel tahlilida Error Level Analysis (ELA) usuli keng qo'llaniladi. Ushbu usul JPEG siqilish darajalaridagi farqlarni aniqlashga yordam beradi. Agar tasvir bir necha marta saqlangan yoki tahrirlangan bo'lsa, ayrim joylarda siqilish darajasi boshqalardan keskin farq qiladi. ELA analizida montaj qilingan qismlar odatda yorqinroq yoki ajralib turuvchi ko'rinishda namoyon bo'ladi. Bu usul ayniqsa qalbaki hujjatlar, o'zgartirilgan suratlar va internetda tarqalgan soxta materiallarni tekshirishda foydali hisoblanadi. Piksel tahlili davomida tasvirdagi shovqin (noise) darajasi ham tekshiriladi. Har bir kamera sensorida o'ziga xos raqamli shovqin mavjud bo'ladi. Original tasvirda bu shovqin butun rasm bo'ylab deyarli bir xil taqsimlangan bo'ladi. Agar tasvirning ma'lum qismi boshqa manbadan olingan bo'lsa, uning shovqin xarakteristikasi farq qiladi. Ekspertlar aynan shu tafovut orqali montaj izlarini aniqlashlari mumkin.

Shuningdek, kontur va chekka qismlarning tekshirilishi ham muhim ahamiyatga ega. Obyekt sun'iy qo'shilganda uning atrofida kesilgan izlar, notabiiy silliqlik yoki xiralik kuzatiladi. Ayniqsa "Photoshop" kabi dasturlar yordamida fon almashtirilgan suratlarda chekka qismlar tabiiy ko'rinmasligi mumkin. Masalan, inson sochi yoki daraxt barglari kabi murakkab shakllarda montaj izlari ko'proq bilinadi.

Ranglar muvozanati ham muhim ekspertiza elementidir. Original tasvirda kamera oq balansni (white balance) avtomatik tarzda moslashtiradi. Agar tasvirning ayrim qismi boshqa suratdan olingan bo'lsa, rang temperaturasi mos kelmaydi. Natijada obyektning rang ohangi fon bilan uyg'unlashmay qoladi. Bu ayniqsa sun'iy yorug'lik yoki quyosh nuri ostida olingan tasvirlarda yaqqol seziladi.

2. Metama'lumotlarni (EXIF) tekshirish

Foto va video tasvirlarning haqiqiylikni aniqlashda metadata tahlili eng muhim raqamli ekspertiza usullaridan biri hisoblanadi. Metadata — bu "ma'lumot haqida ma'lumot" bo'lib, ya'ni faylning ichida yashirin tarzda saqlanadigan texnik va tizimiy ma'lumotlar to'plamidir. Har bir raqamli foto yoki video kamera, telefon yoki dastur orqali yaratilganda avtomatik ravishda metadata hosil bo'ladi. Ushbu ma'lumotlar tasvirning qachon, qayerda va qanday qurilmada yaratilganini aniqlashga yordam beradi. Metadata odatda foydalanuvchiga ko'rinmaydi, lekin maxsus dasturlar yordamida ochiladi. Masalan, EXIF (Exchangeable Image File Format) eng keng tarqalgan metadata formatlaridan biridir. EXIF ma'lumotlari ichida kamera modeli, diafragma (aperture), ISO, ekspozitsiya vaqti, fokus masofasi, sana va vaqt kabi texnik parametrlar saqlanadi. Agar tasvir o'zgartirilgan

bo'lsa, ushbu ma'lumotlarda nomuvofiqliklar paydo bo'lishi mumkin. Metadata tekshiruvda birinchi navbatda faylning yaratilish va o'zgartirilish sanasi tahlil qilinadi. Agar foto 2024-yilda olingan deb ko'rsatilgan bo'lsa, lekin metadata ichida 2022-yil yoki 2026-yil ko'rsatilsa, bu shubhali holat hisoblanadi. Shu bilan birga, fayl "modified" (o'zgartirilgan) va "created" (yaratilgan) vaqtlarining farqi ham muhim ahamiyatga ega. Agar tasvir bir necha marta tahrirlangan bo'lsa, bu vaqtlar orasida katta farq bo'lishi mumkin. Metadata tahlilida kamera yoki qurilma modeli ham katta rol o'ynaydi. Har bir kamera yoki smartfon o'ziga xos EXIF imzosini qoldiradi. Masalan, iPhone, Samsung yoki Canon kameralarining metadata tuzilishi bir-biridan farq qiladi. Agar tasvir oddiy telefon bilan olingan deb ko'rsatilsa, lekin metadata professional kamera parametrlarini ko'rsatsa, bu nomuvofiqlik hisoblanadi. Bu holat ko'pincha internetdan olingan yoki o'zgartirilgan tasvirlarda uchraydi.

GPS ma'lumotlari ham metadata tarkibiga kiradi. Agar kamera yoki telefon joylashuvni aniqlash funksiyasi yoqilgan bo'lsa, tasvir qayerda olingani aniq koordinatalar bilan saqlanadi. Bu sud ekspertizasi va jurnalistik tekshiruvlarda juda muhimdir. Masalan, bir voqea Toshkentda sodir bo'lgan deyilgan bo'lsa, lekin tasvir metadata'si boshqa davlatni ko'rsatsa, bu tasvirning haqiqiylikiga shubha tug'iladi. Biroq shuni ham unutmaslik kerakki, GPS ma'lumotlarini o'zgartirish yoki o'chirish ham mumkin, shuning uchun bu yagona dalil bo'la olmaydi.

Har bir raqamli surat o'zi bilan birga texnik ma'lumotlarni saqlaydi. Nima saqlanadi? Kamera modeli, olingan sana, vaqt, GPS koordinatalar. Qanday tekshiriladi? Internetda bepul bo'lgan "EXIF Viewer" xizmatlari orqali faylni yuklab, uning asl parametrlarini ko'rish mumkin.

3. "Reverse Image Search" (Teskari qidiruv)

Bu usul rasmning internetdagi tarixi va kelib chiqishini aniqlashga yordam beradi. Quyidagi vositalardan foydalanishingiz mumkin:

Vosita nomi	Qanday foydalanish
Google Rasm Qidirish	images.google.com saytiga o'ting, kamera belgisini bosing va rasmni yuklang
TinEye	tineye.com — rasm qayerda va qachon ishlatilganini ko'rsatadi
Yandex Rasmlar	yandex.com/images — rus tilidagi kontentni topishda samarali
Bing Visual Search	bing.com/visualsearch — Microsoft qidiruv tizimi orqali

Agar bu rasm internetda boshqa bir kontekstda yoki ancha avvalroq e'lon qilingan bo'lsa, qidiruv tizimlari sizga asl manbani ko'rsatadi.

Soxta yoki tahrirlangan rasmlarni ko'z bilan aniqlashtirish quyidagi belgilarga e'tibor berish orqali mumkin:

- ✓ Fon bilan old o'rtasidagi chegara noaniq yoki sun'iy ko'rinadi
- ✓ Soyalar noto'g'ri yo'nalishda tushgan yoki umuman yo'q
- ✓ Yorug'lik manbai turli ob'ektlarda bir xil emas
- ✓ Arxitektura yoki tabiiy ob'ektlar geometrik jihatdan noto'g'ri
- ✓ Matn yoki raqamlar noto'g'ri, burilgan yoki o'qib bo'lmaydigan
- ✓ Qo'llar yoki barmoqlar noto'g'ri soni yoki shakli (AI rasmlarida keng tarqalgan)
- ✓ Ko'zoynak shishasidagi aks etish sun'iy ko'rinadi

Videolarning haqiqiylikni tekshirish

Deepfake — bu sun'iy intellekt (AI) va mashinaviy o'rganish (machine learning) algoritmlari yordamida yaratilgan yoki o'zgartirilgan video, audio yoki foto materialdir. Ushbu texnologiya odatda “face swap” (yuz almashtirish), “face reenactment” (yuz harakatini boshqarish) va to'liq sintetik yuz yaratish kabi usullar orqali ishlaydi. Deepfake texnologiyasi kino sanoati, o'yinlar va maxsus effektlarda foydali bo'lishi mumkin bo'lsa-da, u dezinformatsiya, soxta yangiliklar va kiberjinoyatlarda ham keng qo'llanilmoqda. Shu sababli uning belgilarini aniqlash raqamli ekspertizaning eng dolzarb yo'nalishlaridan biridir. Deepfake aniqlash jarayoni bir nechta texnik, vizual va biologik (inson yuziga oid) belgilarni tahlil qilishga asoslanadi. Eng muhim jihatlardan biri — yuz harakatlarining tabiiyligi. Haqiqiy inson yuzida mimika doimiy ravishda murakkab va uzluksiz o'zgarib turadi. Ko'z qimirashi, qosh harakati, lablarning mikromuskul tebranishlari tabiiy fiziologik jarayonlarga bo'ysunadi. Deepfake videolarda esa bu harakatlar ko'pincha silliq emas, ba'zan kechikkan yoki sun'iy ko'rinadi.

Videolarda haqiqiylikni aniqlash murakkabroq, chunki vizual qator bilan birga harakatlar ketma-ketligi ham mavjud.

Deepfake yoki sun'iy yaratilgan videolarda ovoz va lab harakatlari bir-biriga mos kelmasligi mumkin.

Quyidagi belgilar kuzatilishi mumkin:

- gapirish vaqtida lab harakati tabiiy emasligi;
- ovozning robotga o'xshashi;
- talaffuzdagi g'alati pauzalar;
- yuz ifodalarining sun'iy ko'rinishi.

Kontekstual tahlil (Geo-lokatsiya)

Atrof-muhit: Videodagi ob-havo, binolarning arxitekturasini, yo'l belgilari o'sha hududga mos keladimi? Tillar va yozuvlar: Videodagi peshlavhalar yoki yozuvlar qaysi davlat tilida ekanligiga e'tibor bering.

YAKUNLOVCHI QISM — MAVZUNING DOLZARBLIGI

Foto va video tasvirlarning haqiqiylikni aniqlash bugungi raqamli davrda tobora dolzarb ahamiyat kasb etmoqda. Internet, ijtimoiy tarmoqlar va sun'iy intellekt

texnologiyalarining tez rivojlanishi natijasida axborot oqimi keskin oshdi, shu bilan birga soxta yoki manipulyatsiya qilingan vizual materiallar ham ko'payib bormoqda. Ayniqsa deepfake, montaj qilingan videolar va o'zgartirilgan fotosuratlar jamiyatda noto'g'ri fikr shakllanishiga, dezinformatsiya tarqalishiga hamda ijtimoiy ishonchning pasayishiga olib kelishi mumkin.

Mazkur mavzuning dolzarbligi bir necha asosiy omillar bilan izohlanadi. Birinchidan, vizual axborot odamlar tomonidan eng tez ishoniladigan ma'lumot turi hisoblanadi. Ko'pchilik foydalanuvchilar foto yoki videoni ko'rsa, uni avtomatik ravishda haqiqiy deb qabul qiladi. Bu esa soxta kontentning ta'sir kuchini yanada oshiradi. Shu sababli tasvirlarning haqiqiylikni tekshirish mexanizmlarini bilish va qo'llash muhim ijtimoiy ehtiyojga aylanmoqda.

Ikkinchidan, sun'iy intellekt texnologiyalarining rivojlanishi bilan soxta kontent yaratish jarayoni juda osonlashdi. Ilgari murakkab grafik dasturlar va yuqori malaka talab qilingan bo'lsa, hozir oddiy ilovalar yordamida ham realga juda yaqin deepfake videolar yaratish mumkin. Bu esa kiberxavfsizlik, axborot xavfsizligi va huquqiy tizimlar oldiga yangi chaqiriqlarni qo'ymoqda.

Uchinchidan, foto va video dalillar sud-huquq tizimida muhim isbot vositasi hisoblanadi. Agar bunday dalillar soxta bo'lsa, noto'g'ri qarorlar qabul qilinishi ehtimoli oshadi. Shu sababli raqamli ekspertiza usullari, jumladan metadata tahlili, piksel analiz, yorug'lik va soyalar mosligi, hamda fayl strukturasi tekshirish kabi metodlar huquqiy ishonchlilikni ta'minlashda katta rol o'ynaydi.

Shuningdek, jurnalistika va media sohasida ham bu mavzu juda muhimdir. Yangiliklar tez tarqaladigan zamonaviy muhitda har qanday vizual materialning asl yoki soxta ekanligini tekshirish jurnalistlarning professional mas'uliyatiga kiradi. Aks holda noto'g'ri axborot ommaga yetib borishi va keng miqyosda salbiy oqibatlarga olib kelishi mumkin.

Xulosa qilib aytganda, foto va video tasvirlarning haqiqiylikni aniqlash nafaqat texnik jarayon, balki jamiyat axborot xavfsizligining asosiy ustunlaridan biridir. Ushbu sohada bilim va ko'nikmalarga ega bo'lish kiberxavfsizlikni mustahkamlash, dezinformatsiyaga qarshi kurashish hamda ishonchli axborot muhitini yaratishda muhim ahamiyatga ega. Shu sababli bu mavzu hozirgi kunda ham, kelajakda ham o'z dolzarbligini yo'qotmaydi.