# MULTIMEDIA MA'LUMOTLARINING MANIPULYATSIYASINI ANIQLASHDA MASHINALI O'QITISHDAN FOYDALANISH

Assistent **Turdibekov B.B.,**
Toshkent axborot texnologiyalari universiteti, Toshkent

***Annotatsiya:*** *Raqamli dasturiy vositalar bizning kundalik hayotimizning bir qismidir. Ammo tasvirlar va videolarni qayta ishlash uchun dasturiy ta'minotlar tobora kuchliroq va ulardan foydalanish oson bo'lib bormoqda. Bu esa real tasvirlarni soxtalashtirishga imkon beradi. Shunday qilib, so'nggi bir necha yil ichida vizual media kriminalistikasi ajralmas tadqiqot sohasi sifatida paydo bo'ldi, u asosan ko'rib chiqilayotgan raqamli kontentning haqiqiy yoki o'zgarmasligini aniqlashga yordam beradigan vositalar va usullarni ishlab chiqish bilan shug'ullanadi. Mashinali o'qitish tergovchilarga turli xil algoritmlardan foydalangan holda yanada samarali tekshiruvlar o'tkazish imkonini beradi. Har bir mashinali o'qitish algoritmi xususiyatlar asosida raqamli kriminalistikaning ma'lum bir sohasida ishlaydi, u murakkablik, ma'lumotlar hajmi, vaqt oralig'i, korrelyatsiya, izchillik va hokazolarda samaralidir, bundan tashqari, ushbu tadqiqot mashinali o'qitish algoritmlarini standart mezonlar nuqtai nazaridan taqqoslaydi. Shunday qilib, taklif qilingan tizim xato darajasini tahlil qilish usuli orqali tasvirni qayta ishlash bo'yicha neyron tarmog'i kontseptsiyasidan foydalangan holda bunday manipulyatsiya qilingan hujjatlarni aniqlashga yordam beradi,*

***Kalit so'zlar:*** *Raqamli kriminalistika, multimedia kontentini manipulyatsiya qilish; konvolyutsion neyron tarmoqlari; deepfake; raqamli suv belgilari; tasvirlarni qalbakilashtirish; manipulyatsiyani aniqlash, videoni soxtalashtirishni aniqlash; mashinali o'qitish algoritmlari.*

## 1.Kirish

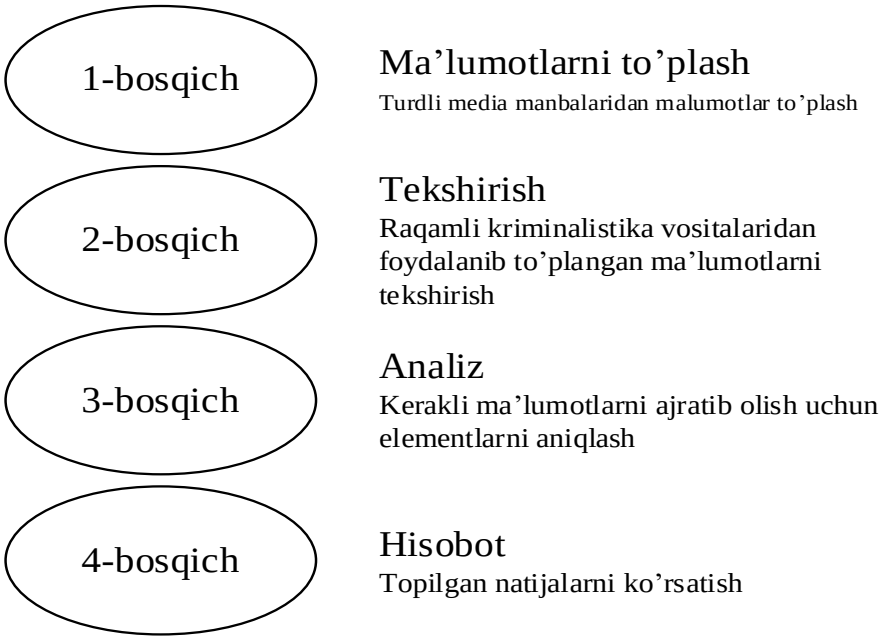
Defacing va deepfakes raqamli fotosuratlar va videolarni buzish uchun multimedia kontentini manipulyatsiya qilish usullaridan foydalanadi. Bu kibertahdidlar kimningdir aytgani va qilayotgan ishlarini o'zgartirish uchun sun'iy intellekt (SI) usullarini qo'llaydigan giperreal videolardan foydalanadi [1]. Ijtimoiy tarmoqlarning keng qamrovliligi va tezligi bilan birlashganda, ishonarli soxta ma'lumotlar tezda millionlab odamlarni o'ziga jalb qilib olishi, umuman jamiyatga

salbiy ta’sir ko‘rsatishi va uning qurbonlari hayotiga haqiqiy vayronagarchiliklarni keltirib chiqarishi mumkin. Deepfake hujumi turli motivlarga ega bo‘lishi mumkin. Soxta yangiliklar [2], pornografik o‘zgartirishlar [3] va raqamli kantentlarni o‘g‘irlashlar, odatda voyaga etmagan yoki boshqa zaif qurbonlar bilan bog‘liq bo‘lgan ransomware shantajlari ular chuqur soxtalik hujumlarining eng dolzarb shakllaridandir. Raqamli kriminalistika tergovchisi tomonidan to‘plangan katta hajmdagi ma’lumotlarni boshqarish uchun ko‘plab usullardan foydalanish mumkin bo‘lsa-da, ular inson miyasi kabi samarali ishlamaydi. Buning o‘rniga, tadqiqotchilar ma’lumotlarni samarali tahlil qilish va to‘plash uchun mashinali o‘qitishdan (ML) foydalanadilar. Ushbu tizim turli misollar va tajribalardan o‘rganishi va ma’lumotlarga asoslanib qaror qabul qilishi mumkin. U Yordam vektor mashinasi (SVM), Qarorlar daraxti (DT), K-Means, K-Nearest Neighbor (KNN), Naive Bayes (NB), Asosiy komponentlar tahlili (PCA), Logistik regressiya (LR), Singular Value Decomposition (SVD) va Apriori kabi turli xil algoritmlarni o‘z ichiga oladi. Har bir algoritm xususiyatlarni ajratib olish, tarmoq hujumlarini tasniflash, manipulyatsiya qilingan tasvirlarni aniqlash va h.k. kabi muayyan vazifa uchun javobgardir[4].

**Raqamli sud ekspertizasi tergov jarayoni**. Raqamli sud ekspertizasi jarayonida qo‘llaniladigan to‘rtta protsedura va metodologiya 2-rasmda ko‘rsatilganidek ishlab chiqilgan. Ular tadqiqotning murakkabligiga qarab turli usullarda amalga oshiriladi. Raqamli texnologiyalarning o‘sishi tufayli to‘planishi mumkin bo‘lgan ma’lumotlar manbalari sonining ko‘payishi kuzatildi. 1-rasmda raqamli kriminalistika ekspertizasini tekshirish jarayoni tasvirlangan. Har bir bosqich quyida tavsiflanadi.

*a) Ma’lumotlarni to‘plash:* Tekshiruvni o‘tkazishning birinchi bosqichi bu ma’lumotlarning potentsial manbalarini aniqlashdir. Odatda, ma’lumotlar noutbuklar, ish stollari va serverlardan yig‘iladi. An’anaviy manbalarga qo‘shimcha ravishda, tahlilchilar tashkilot faoliyatini tahlil qilishda boshqa ma’lumotlar manbalarini ham hisobga olishlari kerak. Masalan, ular Internet-provayderning jurnallari orqali tashkilot faoliyati haqida ma’lumot to‘plashlari mumkin.

*b) Tekshiruv:* Ikkinchi bosqich to‘plangan ma’lumotlarni tekshirishga qaratilgan. Raqamli raqamli kriminalistika texnikasi va vositalaridan foydalanish orqali ma’lumotlardan keraklilari olinadi. Bundan tashqari, siqilgan, kirishni boshqarish va shifrlash orqali yashirilgan ma’lumot fayllari aniqlanadi.

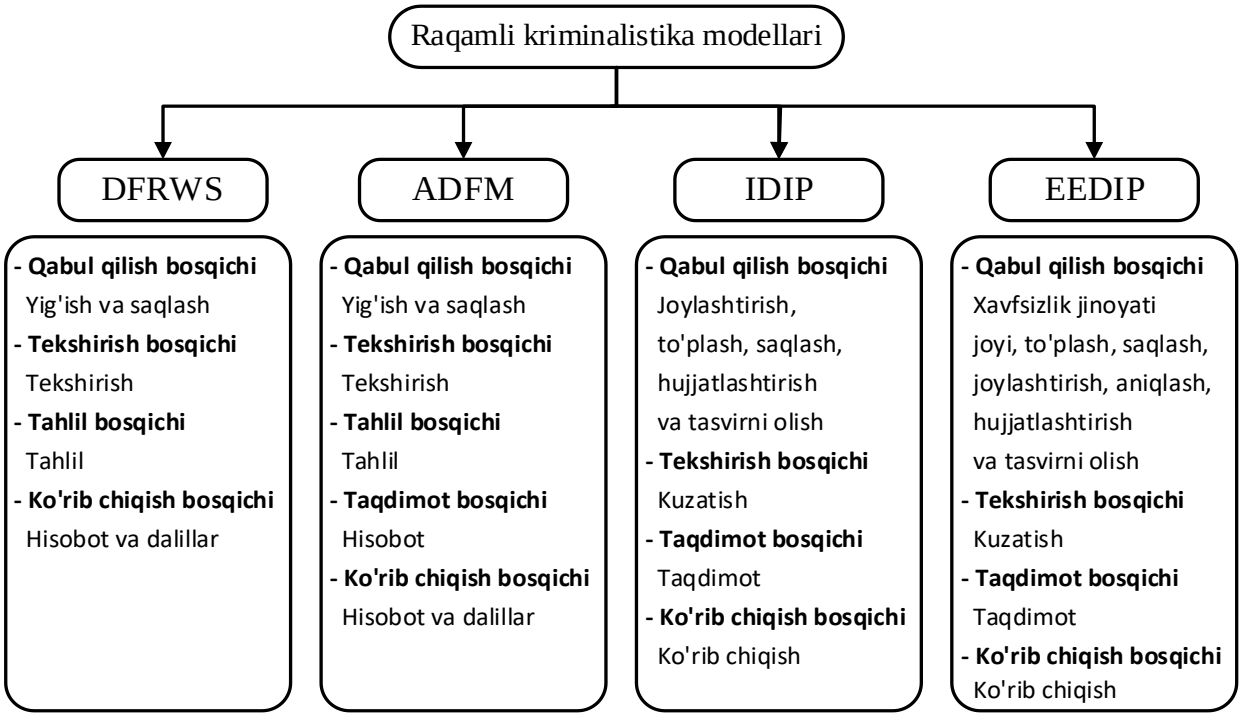



1-rasm. Raqamli sud ekspertizasi tergov jarayoni

*c) Tahlil: Tahlil* - bu odamlar, joylar va hodisalarni aniqlash, shuningdek, bu elementlarning qanday bog‘liqligini aniqlash kabi elementlarni ishlab chiqarish uchun ilmiy sharoitda ilmiy jarayonlarni amalga oshirishni o‘z ichiga olgan jarayondir. Bu jarayon turli manbalardan to‘plangan ma’lumotlarni tahlil qilishni o‘z ichiga oladi.

*d) Hisobot:* Tekshiruvning yakuniy bosqichi hisobot berishdir, bu bosqich tahlil bosqichida to‘plangan ma’lumotlarni tahlil qilishni va xulosalarni tahlilchiga rasmiy hujjatlarda taqdim etishni o‘z ichiga oladi. [5].

**Raqamli sud ekspertizasi modellari.** Raqamli kriminalistika bir nechta tergov modellariga ega, masalan, Raqamli kriminalistika ekspertizasi seminarlari modeli (DFRWS), mavhum raqamli kriminalistika modeli (ADFM), integratsiyalangan raqamli tergov jarayoni modeli (IDIP) va end-to-end raqamli tergov jarayoni modeli (EEDIP). Har bir model ma’lum bir bosqich va faoliyat uchun mo‘ljallangan. 2-rasmda tegishli faoliyat bilan raqamli kriminalistika modellari ko‘rsatilgan. Sun’iy intellektga (AI) eng keng tarqalgan yondashuvlardan biri bu tizimlarni qo‘shimcha treningni talab qilmasdan o‘qitish va tahlil qilish imkonini beruvchi mashinali o‘qitishdir. U qabul qilingan ma’lumotlarni avtomatik ravishda tasniflashi va bashorat qilishi mumkin [6].




2-rasm. Raqamli kriminalistika modellari

Mashinali o‘qitish to‘rtta asosiy toifaga bo‘linadi: o‘qituvchili o‘qitish, o‘qituvchisiz o‘qitish, yarim o‘qituvchili o‘qitish va mustahkam o‘qitish.O‘qituvchili o‘qitish jarayoni misollari kirishni chiqish bilan taqqoslaydi. U turli o‘qitish misollari bilan belgilangan o‘quv ma’lumotlaridan foydalanadi. Regressiya va tasniflash bu jarayonda qo‘llaniladigan eng mashhur usullardir[4].

Machine Learning (ML) raqamli kriminalistika vositalari uchun raqamli artefaktlarni avtomatlashtirilgan aniqlash va tasniflashni kuchaytiradi. Manipulyatsiya qilingan fotosuratlar va videolarni aniqlash uchun mavjud ML texnikasi [7] kamdan-kam hollarda raqamli kriminalistika ilovalariga qo‘shilmaydi. Shuning uchun chuqur soxta ma’lumotlarni aniqlashga qodir bo‘lgan ML-ga asoslangan Autopsy modullari dolzarbdir va ular, albatta, tergov organlari tomonidan juda yuqori baholanadi. Soxta ma’lumotlarni aniqlash bo‘yicha xabar qilingan ML usullarida kuzatilgan yaxshi natijalar hali kiberjinoyatlarni tergov qilish uchun sezilarli yutuqlarga to‘liq erishilmagan. [8].

Raqamli kriminalistika tergovchisi tomonidan to‘plangan katta hajmdagi ma’lumotlarni boshqarish uchun ko‘plab usullardan foydalanish mumkin bo‘lsa-da, ular inson miyasi kabi samarali ishlamaydi. Ma’lumotlarni samarali tahlil qilish va to‘plash uchun mashinali o‘qitishdan (ML) foydalanish samarali hisoblanadi. Ushbu tizim turli misollar va tajribalardan o‘rganishi va ma’lumotlarga asoslanib qaror qabul

qilishi mumkin. U Yordam vektor mashinasi (Support Vector Machine - SVM), K-Means, K-Nearest Neighbor (KNN), Naive Bayes (NB), Asosiy komponentlar tahlili (PCA), Qarorlar daraxti (DT), Singular Value Decomposition (SVD), Logistik regressiya (LR) va Apriori kabi turli xil algoritmlarni o‘z ichiga oladi. Algoritmlar xususiyatlarni ajratib olish, tarmoq hujumlarini tasniflash, manipulyatsiya qilingan tasvirlarni aniqlash va h.k. kabi muayyan vazifalar uchun foydalaniladi[4].

Mashinalarni o‘qitish kiberxavfsizlik va raqamli kriminalistikada muhim rol o‘ynaydi. Raqamli kriminalistika tergovchilari turli xil bulutli hisoblash muhitlari va tarmoqlarida saqlangan katta hajmdagi ma’lumotlar to‘plamlarini tahlil qilish uchun mashinali o‘qitish algoritmlaridan foydalanadilar. Ushbu ma’lumotlar to‘plamlari keyinchalik foydalanuvchilarning xatti-harakatlarini bashorat qilish uchun ishlatiladi. Mashinali o‘qitish usullaridan foydalanish orqali tergovchilar potentsial jinoiy faoliyatni aniqlash uchun ma’lumotlar namunalarini topish uchun ishlatilishi mumkin bo‘lgan bir qator qoidalar va usullarni qo‘llaydilar. 1-jadvalda raqamli dalillarni topish uchun taklif qilingan bir nechta algoritmlar tavsiflangan.

Jadval 1. Raqamli kriminalistika tekshiruvida mashinali o‘qitish algoritmlarining qisqacha mazmuni.

| Fokus maydoni | ML Algoritmi | Kriminalistika turi | RK Fazasi | Afzalliklari | Kamchiliklari |
|---|---|---|---|---|---|
| **Nusxa ko‘chirish-ko‘chirish va ulash hujumlar** | SVM | Tasvir kriminalistikasi | Tekshiruv | Yuqori aniqlik va o‘qitilgan ma’lumotlar to‘plami | Bir-biriga o‘xshash tasvirlarda kamroq ishlatilishi |
| **Kontrastni yaxshilash va JPEG-siqilgan tasvirni aniqlash** | SVM | Tasvir kriminalistikasi | Tekshiruv | Tez ma’lumotlarni tahlil qilish | Detektor (QF) faqat ma’lum bir QFda yaxshi ishlaydi |
| **Manipulyatsiya qilingan video va fotosuratlarni aniqlash** | SVM | Tasvir va video kriminalistikasi | Tahlil | Yuqori aniqlik | Ko‘proq ishlov berish vaqti talab qilinadi |
| **Manba klassifikatsiyasi** | RF, KNN, RF, AB, SVM | Video kriminalistikasi | Tekshirish va tahlil qilish | Qorong‘i videolarda yuqori aniqlik | Prognoz bosqichida past ishlash |
| **Tasvir manbasini aniqlang** | PCA, RF | Tasvir kriminalistikasi | Tekshiruv | Aniqlik yuqori va xususiyatlarning o‘lchami kam | Komponentlar to‘g‘ri o‘rnatilmagan bo‘lsa, ma’lumotlar yo‘qoladi |
| **Tasvirni soxtalashtirish** | SVD | Tasvir kriminalistikasi | Tekshirish va tahlil qilish | Yuqori aniqlik | Past sifatli tasvirdagi blok hajmini kamligi |
| **Tasvirlarda nusxa ko‘chirish va qalbakilashtirish** | SVD | Tasvir kriminalistikasi | Tahlil | Yuqori unumdorlik va kamroq hisoblash | - |

Ushbu maqola raqamli fotosuratlar, shuningdek, manipulyatsiya qilingan va deepfake hujumining bir qismi bo‘lishi mumkin bo‘lgan videolarni aniqlash uchun mustaqil dasturni o‘rnatish va ishlab chiqishni tasvirlaydi. Ilova Autopsy uchun ikkita alohida modul sifatida, ya’ni manipulyatsiya qilingan raqamli fotosuratlar va boshqa manipulyatsiya qilingan videolarni aniqlash uchun joylashtirildi. Mustaqil dastur va Autopsy uchun ishlab chiqilgan Python modullari o‘z ichiga oladi

**Tasvir va video fayllarni soxtalashtirish**

Tasvirning soxtaligini ma’lum bir semantik o‘zgartirish sifatida aniqlanadi. Kontrastlarning sozlanishi yaxshilanish deb ataladi, rang o‘zgarishi esa soxtalik deb hisoblanadi.

Videoni uch o‘lchovli tasvir sifatida ko‘rish mumkin, bu erda uchinchi o‘lchov vaqtdir. Video qalbakilashtirish videoning tarkibini fazoviy (x va y o‘lchami) yoki vaqt o‘lchamini o‘zgartirishdan iborat. Fazoviy video qalbakilashtirishni bir nechta kadrlarga qo‘llaniladigan oddiy tasvir soxtalashtirish sifatida ko‘rish mumkin. Tasvir va fazoviy video soxtalashtirishning to‘rtta asosiy toifaga [9] ajratish mumkin. Aniqlash nuqtai nazaridan, har qanday vaqtga asoslangan soxtalikni ikki toifaga bo‘lish mumkin [10]: kadrni o‘chirish va freymni kiritish.

**Birlashtirish soxtalashtirishi.** Eng keng tarqalgan soxtalashtirish Splicing deb ataladi. Soxtalashtirish kamida ikkita rasmni o‘z ichiga oladi, ular manba tasvirlari va maqsadli tasvir deb ataladi. Birlashtirish manba tasvirlaridan maqsadli tasvirga bir yoki bir nechta elementlarni kiritishdan iborat. O‘rnatilgan elementlar to‘g‘ri joylashtirish uchun o‘zgartirilishi mumkin. Shunisi e’tiborga loyiqki, bu hozirgacha qilish mumkin bo‘lgan eng murakkab soxtalashtirishdir. Haqiqatan ham, ishonchli birlashma ishlab chiqarish uchun qalbakilashtiruvchi yorug‘lik, kiritilgan elementning ko‘rish burchagi, uning aniqligi va boshqalarga mos kelishi kerak. Hatto eng kichik mos kelmaslik ham birlashmani butunlay soxta ko‘rinishiga olib kelishi mumkin.

**Nusxalash-ko‘chirish soxtalashtirish.** Boshqa soxtalashtirishlardan farqli o‘laroq, nusxa ko‘chirish faqat bitta tasvirni o‘z ichiga oladi. Nusxalash-ko‘chirish soxtalashtirishda bir manba ko‘chiriladi va boshqa kontentga biriktiriladi. Takrorlangan elementni tarjima qilish, aylantirish, o‘zgartirish mumkin. Nusxa ko‘chirish soxtaligini yaratish odatda soxtalashtirishdan ko‘ra osonroqdir. Garchi u juda cheklangan bo‘lib ko‘rinsa ham, aslida u juda ko‘p qirrali. Miqdorni aldash, elementni yashirish yoki matn maydonini o‘zgartirish uchun nusxa ko‘chirishdan foydalanish mumkin.

**Ob’ektni olib tashlash qalbakilashtirish.** Ob’ektni olib tashlash faqat bitta tasvirga ishlov berishni o‘z ichiga oladi. Ob’ektni olib tashlash tasvirdan bitta elementni yo‘qotishdan iborat. Bunday qalbakilashtirish nusxa ko‘chirish yordamida

amalga oshirilishi mumkin, ammo bu soxtalikni yaratishning boshqa usullari mavjud. Xususan, ob'ektni olib tashlash ko'pincha inpainting algoritmi yordamida amalga oshiriladi. Namunaga asoslangan, diffuziyaga asoslangan, chuqur o'rganishga asoslangan rasmga ishlov berish usullarining ko'p turlari mavjud [11].

**Yuz manipulyatsiyasi.** Aytish mumkinki , bular shunchaki yuz tasvirlariga qo'llaniladigan soxtalashtirish usulidir. Ba'zi yuz manipulyatsiyalari samarali ravishda oddiygina bog'lanishdir, ammo ular haqiqatan ham yuz tasvirlari uchun xos bo'lganligi sababli, ular qalbakilashtirishga oddiy birlashmadan tashqari qo'shimcha usullardan foydalanishga imkon beradi. Eng oddiy va eng mashhur yuz manipulyatsiyasi yuzni almashtirish deb ataladi. Yuzni almashtirish - bu bir yuzni boshqasiga oddiy birlashtirish. Chuqur neyron tarmoqlarning rivojlanishi bilan endi hatto videolarda ham juda real yuz almashinuvini yaratish mumkin. Ushbu dinamika yuzlarini almashtirish usullari ko'pincha DeepFakes deb ataladi. Ular, odatda, haqiqiy yuz o'rniga soxta yuzni sintez qilish uchun chuqur neyron tarmoq yordamida almashtirishni amalga oshiradilar, shuning uchun DeepFakes deb nomlanadi[12].

**Kadrni o'chirish.** Kadrni o'chirish video qalbakilashtirishga xosdir. Nomidan ko'rinib turibdiki, u bir yoki bir nechta kadrlarni olib tashlashdan iborat. O'chirilgan qism videoning istalgan joyida bo'lishi mumkin. Odatda videoning yashirin qismlaridan foydalaniladi. Misol uchun, qalbaki pul sotuvchisi o'zi paydo bo'lgan kuzatuv videosini buzishni xohlashi mumkin. Shunday qilib, u o'zi ko'rinadigan har bir kadrni olib tashlaydi.

**Kadr kiritish.** Kadrni kiritish esa video ichiga yangi kadrlar qo'shishdan iborat. Ushbu yangi kadrlar bir xil yoki boshqa videodan olinishi mumkin. Bunday soxtalashtirish uchun asosiy foydalanish bir nechta ketma-ketlikdan iborat video kompozitsiyani yaratishdir. Bundan tashqari, videoning olib tashlangan qismini to'ldirish uchun kadr o'chirish soxtaligi bilan bir qatorda foydalanish mumkin.

**Videoni qalbakilashtirish.**

Raqamli kameralar va mobil telefonlar va portativ videotasvirga olish qurilmalarining keng tarqalishi kuzatuv kameralaridan foydalanishning o'sishi multimedia ma'lumotlarining keskin kopayishiga olib keldi. Raqamli tasvirlar va videolar mazmuni tomonidan taqdim etilgan ma'lumotlar jinoiy yoki kriminal, razvedka xizmatlari, siyosat va jurnalistika sohalarida muhim qarorlar uchun asos bo'ladi. Masalan, jinoiy sud jarayonida jinoyatning kuzatuv kameralari tasvirlari "video dalil" sifatida ko'rsatilishi mumkin va uning mazmuni voqeani to'g'ri tasvirlashni ta'minlaydi.

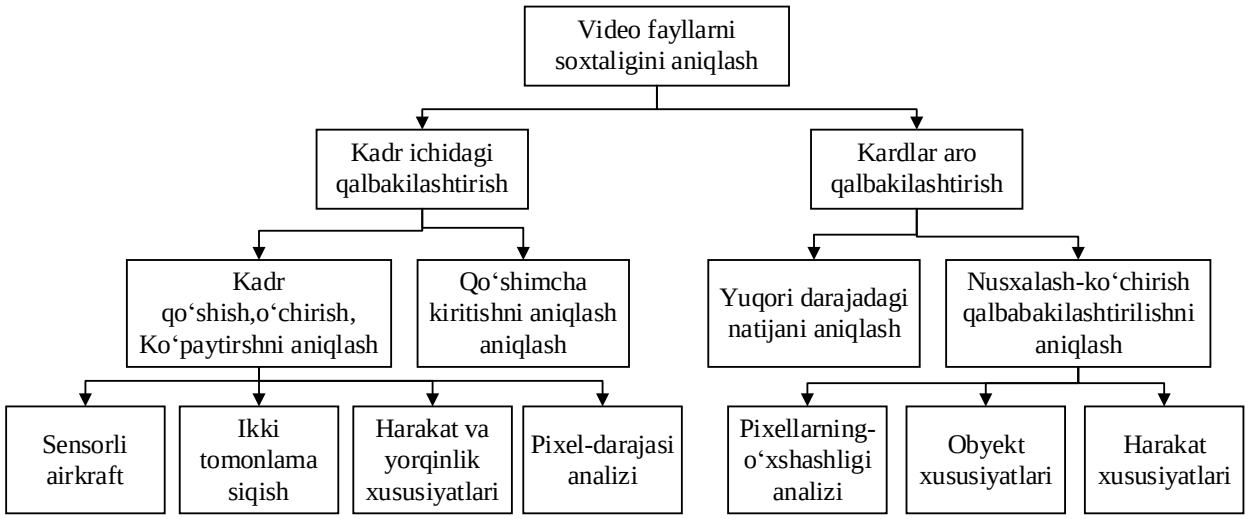
Adobe Premiere, Photoshop, Cinelerra va Lightworks kabi video tahrirlash uchun qulay dasturlarning keng tarqalganligi va ixtisoslashtirilgan qalbakilashtirish

usullarining rivojlanishi soxta raqamli videolarning hosil bo‘lishiga olib keldi [13], Oddiy foydalanuvchi ham raqamli videolar mazmunini ularni haqiqiy kontentdan deyarli farqlanmaydigan qilib o‘zgartirishga qodir. Video qalbakilashtirishning bir nechta turlari mavjud, lekin ularning barchasi odatda ikkita toifadan biriga tegishli bo‘ladi: kadrlararo qalbakilashtirish yoki ichki qalbakilashtirish[14].

*(a) Kadrlararo qalbakilashtirish*. Bu qandaydir yo‘l bilan videodagi kadrlar ketma-ketligiga ta’sir qiluvchi qalbakilashtirish turlari. Odatda, bunday soxtalashtirishlar video ketma-ketlikdan yoki undan kadrlar to‘plamini olib tashlash yoki kiritishni o‘z ichiga oladi. Kadrlarni takrorlash shuningdek, kadrlar to‘plamidan nusxa ko‘chirish va boshqa vaqtinchalik joyda bir xil videoga kiritish interframe qalbakilashtirishning bir turi hisoblanadi. Bunday qalbakilashtirishlarni "freymlararo nusxa ko‘chirish-joylashtirish" deb ham atash mumkin. Kadrlararo qalbakilashtirishning yana bir turi - vaqtinchalik birlashma bo‘lib, yangi video yaratish uchun ikki yoki undan ortiq turli videolarning kadrlari interpolyatsiya qilinadi.

*(b) Kadr ichidagi qalbakilashtirish.* Kadr ichidagi qalbakilashtirishda alohida kadrlarning haqiqiy mazmuni o‘zgartiriladi. Nusxa ko‘chirish-joylashtirish va yuqori darajali kesish kadr ichidagi soxtalashtirishga misoldir.

3-rasmda video fayllarni qalbakilashtirish va ularni aniqlash usullarining turkumlanishi keltirilgan.

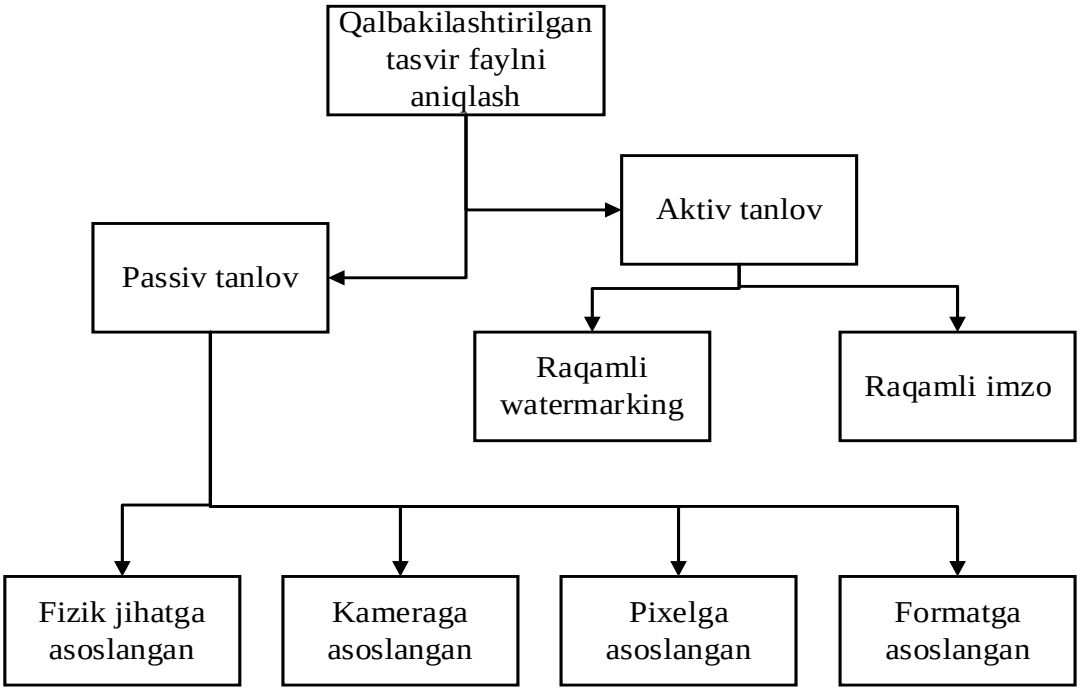



3- rasm. Video fayllarni qalbakilashtirishni aniqlash usullarini turkumlash.

**Rasmlarni soxtalashtirish.**

Tasvirning soxtaligini aniqlash usullarining ko‘p turli toifalari mavjud. Ushbu toifalarning umumiy ko‘rinishini 4-rasmda ko‘rish mumkin. Asosan ikkita asosiy tasvir soxtaligini aniqlash oilalarini ko‘rish mumkin. Passiv yondashuv va faol yondashuv[12]. Faol yondashuvni ikkita asosiy oilaga bo‘lish mumkin. Bular Watermarking va kriptografiyadan foydalanish usullariga asoslangan yondashuvlardir. Ikkala oilaning ham g‘oyasi ommaviy axborot vositalariga o‘zgartirib bo‘lmaydigan

element qo‘shishdir. Bu ommaviy axborot vositalaridan foydalanish imkoniyatiga ega bo‘lishni va o‘sha paytda ommaviy axborot vositalarining haqiqiyligiga ishonch hosil qilishni talab qiladi.




4-rasm. Tasvir soxtaligini aniqlash bo‘yicha umumiy ko‘rinish.

Suv belgisini kiritish uchun piksel ma’lumotlaridan foydalaniladi. Suv belgisi tasvirning yuqori qismidagi aniq yoki ko‘rinmas matn bo‘lishi mumkin. Kriptografiyaga asoslangan yondashuvlar piksel ma’lumotlarini o‘zgartirmaydi. Buning o‘rniga, media shifrlash algoritmi yordamida shifrlanadi, shuning uchun uni shifrlash kalitini bilmasdan o‘zgartirib bo‘lmaydi. Yoki u raqamli imzo bilan imzolanishi mumkin, shuning uchun har qanday o‘zgarishlar buzilgan media va imzo o‘rtasidagi nomuvofiqlik bilan aniqlanadi. Boshqa tomondan, passiv yondashuvlar tasvirni shakllantirish yoki buzish jarayoni haqidagi taxminlar haqidagi bilimlarga asoslanadi.

**Xulosa**

Raqamli kriminalistika ekspertlari jarayonlarni aniqlashga yordam beradigan tasvirlar, videolar va boshqalar kabi katta ma’lumotlarni tahlil qilishda har bir holatda ko‘plab qiyinchiliklarga duch kelishlarini isbotladilar. Vaqt o‘tishi bilan raqamli kriminalistikaotida ba’zi yangi muammolar paydo bo‘ladi. Bu tergovchilarning ishini osonlashtiradigan avtomatlashtirish va aqlli texnikalardan foydalanishga olib keldi. Ushbu tadqiqot raqamli kriminalistika muammolarni hal qilish uchun turli ML algoritmlarini tasdiqladi, masalan, SVM, KNN, DT, PCA, SVD, K-Means, NB, ANN, LR va RF. Algoritmlar sudda dalillar uchun soxta ma’lumotlardan haqiqiy

ma’lumotlarni tasniflaydi. Har bir multimediya faylida DFT hisob-kitobi natijasida olingan avval chiqarilgan xususiyatlarni qayta ishlash uchun SVM-ga asoslangan usul mustaqil dasturda amalga oshirildi. Autopsy raqamli kriminalistika vositasi uchun ikkita modul ishlab chiqilgan, ya’ni o‘zgartirilgan fotosuratlarni aniqlash moduli va boshqasi chuqur soxta videolarni aniqlash uchun. Raqamli kriminalistikaoti, SVM va DFT asoslari tavsiflangan. Multimedia kontenti bo‘yicha raqamli sud ekspertizasi bilan bog‘liq eng dolzarb va dolzarb adabiyotlar ko‘rib chiqildi, ya’ni fotosuratlar va video ekspertizasiga qo‘llaniladigan chuqur o‘rganishga asoslangan usullar. Ushbu tadqiqot natijasida olingan natijalar modullari raqamli sud ekspertizasi tergovchilariga yordam qo‘lini beradi va multimedia fayllarini o‘z ichiga olgan kiberjinoyatlarga qarshi kurashish uchun ML texnikasidan foydalanadi. Umumiy arxitektura va ishlanma multimedia tarkibidagi xususiyatlarni ajratib olish va o‘rganish klassifikatorlari modellarini avtomatik ravishda aniqlash uchun ikkita taniqli va hujjatlashtirilgan texnikadan foydalanadi, mos ravishda fotosuratlardan xususiyatlarni ajratib olish uchun Diskret Furye Transformasi (DFT) texnikasi va SVM. Noto‘g‘ri tasniflangan fotosuratlar va video kadrlarni tahlil qilish orqali, mumkin bo‘lgan sabab fotosuratlarning past aniqligi bilan bog‘liq bo‘lishi mumkin. Fotosuratlardan olinishi kerak bo‘lgan xususiyatlarning optimal soni va uning hisoblash vaqtidagi ta’siri ham o‘rganishga arziydi. Ham chuqur o‘rganish, ham SVMga asoslangan usullardan tashkil topgan o‘quv tasniflagichlari ansambli olingan samaradorlik va ishlov berish vaqtidan foyda keltirishi mumkin. CNN yordamida, oxir-oqibat boshqa arxitekturadan foydalangan holda raqamli kriminalistikani aniqlashning aniq modeli ham tadqiq qilish va amalga oshirish uchun arziydi.

## ADABIYOTLAR

1. Westerlund M (2019) The emergence of deepfake technology: A review. Technology Innovation Management Review 9:39–52. https://doi.org/10.22215/TIMREVIEW/1282

2. (PDF) Fake News and Deepfakes: A Dangerous Threat for 21st Century Information Security. https://www.researchgate.net/publication/341454354_Fake_News_and_Deepfakes_A_Dangerous_Threat_for_21st_Century_Information_Security. Accessed 5 May 2023

3. Harris DA (2019) Deepfakes: False Pornography Is Here and the Law Cannot Protect You. Duke Law Technol Rev

4. Balushi Y Al, Shaker H, Kumar B (2023) The Use of Machine Learning in Digital Forensics: Review Paper. Proceedings of the 1st International Conference on

Innovation in Information Technology and Business (ICIITB 2022) 96–113. https://doi.org/10.2991/978-94-6463-110-4_9

5. Costantini S, De Gasperis G, Olivieri R (2019) Digital forensics and investigations meet artificial intelligence. Ann Math Artif Intell 86:193–229. https://doi.org/10.1007/S10472-019-09632-Y/METRICS

6. Dhall D, Kaur R, Juneja M (2020) Machine learning: A review of the algorithms and its applications. Lecture Notes in Electrical Engineering 597:47–63. https://doi.org/10.1007/978-3-030-29407-6_5/COVER

7. Tolosana R, Vera-Rodriguez R, Fierrez J, et al (2020) Deepfakes and beyond: A Survey of face manipulation and fake detection. Information Fusion 64:131–148. https://doi.org/10.1016/J.INFFUS.2020.06.014

8. Bhatt P (2017) MACHINE LEARNING FORENSICS:A NEW BRANCH OF DIGITAL FORENSICS. International Journal of Advanced Research in Computer Science 8:217–222. https://doi.org/10.26483/IJARCS.V8I8.4613

9. Verdoliva L (2020) Media Forensics and DeepFakes: An Overview. IEEE Journal on Selected Topics in Signal Processing 14:910–932. https://doi.org/10.1109/JSTSP.2020.3002101

10. Shelke NA, Kasana SS (2021) A comprehensive survey on passive techniques for digital video forgery detection. Multimed Tools Appl 80:6247–6310. https://doi.org/10.1007/S11042-020-09974-4/TABLES/10

11. Joshi P, Shrivastav N (2018) A Review Paper on Image Inpainting and their Different Techniques. Asian Journal of Computer Science and Technology 7:108–111. https://doi.org/10.51983/AJCST-2018.7.1.1821

12. Mahfoudi G (2021) Authentication of Digital Images and Videos. http://www.theses.fr

13. Pic MM, Mahfoudi G, Trabelsi A, Dugelay JL (2022) Face Manipulation Detection in Remote Operational Systems. Advances in Computer Vision and Pattern Recognition 413–436. https://doi.org/10.1007/978-3-030-87664-7_19/FIGURES/8

14. Ferreira S, Antunes M, Correia ME (2021) A Dataset of Photos and Videos for Digital Forensics Analysis Using Machine Learning Processing. Data 2021, Vol 6, Page 87 6:87. https://doi.org/10.3390/DATA6080087