Razvoj i primjena IP sustava videonadzora

Dončević, Dominik

SVEUČILIŠTE U RIJECI

TEHNIČKI FAKULTET

Diplomski sveučilišni studij elektrotehnike

Diplomski rad

RAZVOJ I PRIMJENA IP SUSTAVA VIDEONADZORA

Rijeka, rujan 2023.

Dominik Dončević

0036495488

SVEUČILIŠTE U RIJECI

TEHNIČKI FAKULTET

Diplomski sveučilišni studij elektrotehnike

Diplomski rad

RAZVOJ I PRIMJENA IP SUSTAVA VIDEONADZORA

Mentor: Prof. dr. sc. Nino Stojković

Rijeka, rujan 2023.

Dominik Dončević

0036495488

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
POVJERENSTVO ZA DIPLOMSKE ISPITE

Rijeka, 15. ožujka 2023.

Zavod: **Zavod za automatiku i elektroniku**
Predmet: **Analogna obrada signala**
Grana: **2.03.03 elektronika**

ZADATAK ZA DIPLOMSKI RAD

Pristupnik: **Dominik Dončević (0036495488)**
Studij: Sveučilišni diplomski studij elektrotehnike
Modul: Automatika

Zadatak: **Razvoj i primjena IP sustava video nadzora / Development and implementation of IP system for video surveillance**

Opis zadatka:

Potrebno je opisati razvoj i primjenu tehnologije IP (Internet protokol) video nadzora. Navesti prednosti i nedostatke u odnosu na zastarjeli analogni video nadzor. Obraditi osnovne komponente IP mreže, karakteristike samog video nadzora kao i centralnu opremu. Opisati specijalne funkcije i analitiku video nadzora. Prikazati primjer izrade cjelokupnog projekta na fizičkoj lokaciji, odraditi potrebne izračune i priložiti dokumentáciju. Za dodatne informacije javiti se mentoru.

Rad mora biti napisan prema Uputama za pisanje diplomskih / završnih radova koje su objavljene na mrežnim stranicama studija.

Zadatak uručen pristupniku: 20. ožujka 2023.

Mentor:

Prof. dr. sc. Nino Stojković

Predsjednik povjerenstva za diplomski ispit:

Prof. dr. sc. Dubravko Franković

IZJAVA

Sukladno s pravilnikom o diplomskom radu, diplomskom ispitu i završetku diplomskih sveučilišnih studija, izjavljujem da sam diplomski rad na temu „Razvoj i primjena IP sustava videonadzora“ izradio samostalno uz pomoć mentora iz firme Alarm Automatika d.o.o. uz svu potrebnu literaturu.

Dominik Dončević

Rijeka, rujan 2023.

ZAHVALA

Zahvaljujem se svom mentoru dr.sc.prof. Ninu Stojkoviću na pruženoj prilici da diplomski rad napravim u sklopu firme u kojoj radim koji mi je uvelike utjecao na proširivanje potrebnog znanja. Posebno se zahvaljujem svojim roditeljima, prijateljima i budućoj zaručnici na podršci i strpljenju u svim trenucima kroz cijelo vrijeme studiranja.

SADRŽAJ

1. UVOD

Tehnologija IP videonadzora značajno je napredovala u pogledu kvalitete slike, kapaciteta pohrane podataka i jednostavnosti upotrebe. Sustavi IP videonadzora prvi su se puta pojavili u 1990. godini i prvotno su se koristili uglavnom u velikim tvrtkama i vladinim organizacijama. Ti su sustavi bili skupi i zahtijevali su specijaliziranu opremu i stručnost za postavljanje i rad. Osim toga, uvođenje IP videonadzora često je zahtijevalo nadogradnju postojeće mrežne infrastrukture kako bi se podržao prijenos visokokvalitetnih videozapisa što je dodatno povećavalo troškove i složenost implementacije. Međutim, s napretkom tehnologije i sve većom rasprostranjenošću IP videonadzora cijene su se smanjile, a sustavi su postali jednostavniji za montiranje, reguliranje i primjenu uz značajno poboljšanje kvalitete slike i mogućnosti nadzora. Danas je IP sustav videonadzora prisutan u svim vrstama okruženja, različitim industrijskim postrojenjima, zdravstvenim i obrazovnim ustanovama, poslovnim i turističkim objektima, prometnoj infrastrukturi te mnogim privatnim domovima. U ovom radu istražit će se razvoj i primjena IP videonadzora, opisati i analizirati fizičke i programske komponente takvog sustava te razmotriti izazove koji proizlaze iz njegove svakodnevne primjene.

2. ZAŠTITA OSOBNIH PODATAKA

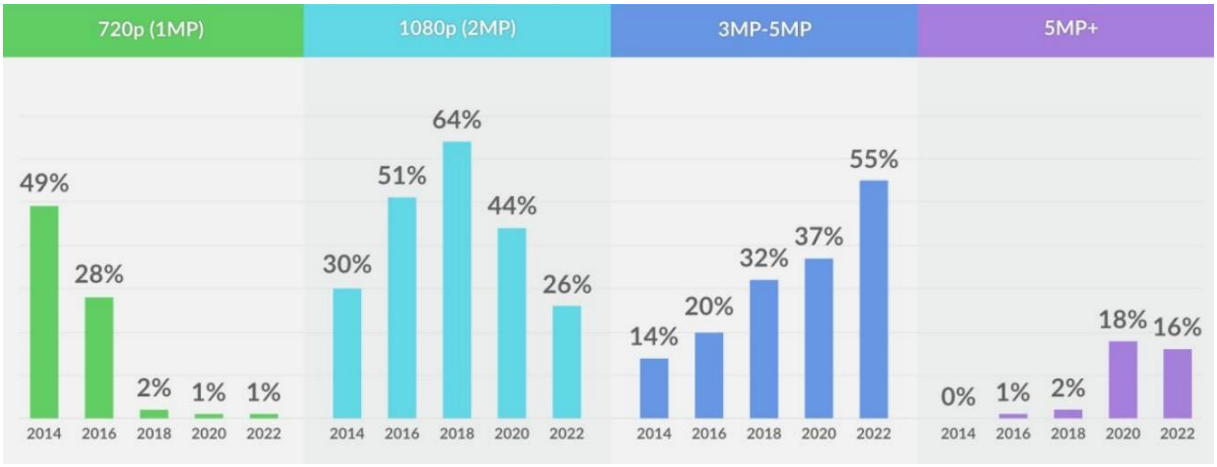
Opća uredba o zaštiti podataka Europske Unije ili GDPR (eng. General Data Protection Regulation) važan je zakon koji regulira obradu osobnih podataka građana EU, uključujući i podatke prikupljene putem sustava videonadzora. U tom slučaju, potrebno je pridržavati se odredbi GDPR-a kako bi se zaštitila privatnost pojedinca čiji se podaci mogu prikupiti i koristiti. Potrebno je imati legitimnu pravnu osnovu za prikupljanjem i obradom osobnih podataka koja se može ostvariti pri izvršavanju ugovora, ispunjavanju pravne obveze ili na temelju suglasnosti. Osobe koje su pod videonadzorom trebaju biti obaviještene o postojanju takve vrste nadzora, svrsi i trajanju obrade podataka te fizičkim ili pravnim osobama koje imaju pristupa tim podacima. Osobni podaci prikupljeni putem videonadzora moraju se čuvati sigurno i ne dulje nego što je potrebno za svrhu za koju su prikupljeni. Vrijeme zadržavanja ovisi o svrsi, pravnim obvezama i politikama zadržavanja podataka. Također, pojedinci imaju pravo na pristup, ispravak, brisanje, prigovor i prenosivost podataka te se njihovo pravo uvijek mora zadovoljiti. Iz tog razloga, potrebno je osigurati odgovarajuće tehničke i organizacijske mjere kako bi se zaštitili osobni podaci od neovlaštenog pristupa ili otkrivanja. U slučaju da je videonadzor visokorizičan za prava pojedinaca (npr. veliki javni prostor), nužno je provesti analizu utjecaja na zaštitu podataka ili DPIA (eng. Data Protection Impact Assessment) kako bi se procijenili potencijalni rizici i poduzele mjere njihovog smanjenja. Od velike je važnosti održavati dokumentaciju o aktivnostima vezanim uz obradu osobnih podataka putem videonadzora kako bi se mogla dokazati usklađenost s GDPR-om u slučaju inspekcije ili pritužbi. [1]

3. POVIJEST RAZVOJA VIDEONADZORA

Tržište videonadzora značajno se mijenjalo tijekom posljednjih 20 godina, počevši od videorekordera sve do umjetne inteligencije i pohrane podataka u oblaku (eng. cloud). Početkom 2000-ih dolazi do masovnog proboja mrežnog snimača ili DVR-a na tržište (eng. Digital Video Recorder) koji su zamijenili tada korištene videorekordere. Prednosti DVR-a u odnosu na videorekordere zamjena su tada skupih i glomaznih VHS kazeta (eng. Video Home System) digitalnim snimanjem kao i mogućnost upravljanja i praćenja videonadzora pomoću IP (eng. Internet Protocol) mreže. S obzirom na ograničenu pohranu i nisku rezoluciju, DVR je i dalje bio poprilično skup, ali jeftiniji od operativnih troškova održavanja VHS kazeta. Daljinsko praćenje bilo je moguće uz ograničeno komprimiranje i brzinu prijenosa podataka što je uzrokovalo lošom kvalitetom i brzinom videonadzora. Krajem 2001. godine, ponajviše nakon 9. rujna, došlo je to osjetnog porasta potražnje za videonadzorom. Takav trenutni porast rezultirao je povećanim interesom za razmatranjem novih i skupljih tehnologija, ali isto tako i nepromišljene kupnje slabo testiranog i nedovoljnog zrelog sustava. Sve do 2008. godine industrijom su dominirali DVR-ovi i SD (eng. Standard Definition) analogne kamere dok se nije usvojilo napredno video kodiranje poznato kao H.264 ili MPEG-AVC (eng. Advanced Video Coding). To je dovelo do učestalijeg korištenja megapikselnih IP kamera i VMS programske podrške (eng. Video Management Software) zbog mogućnosti pružanja bolje razlučivosti s razumnim povećanjem ukupnih troškova. Zajedno s porastom megapikselnih IP kamera pojavio se i značajan interes u povezivanju tih kamera s oblakom u svrhe uklanjanja potrebe za održavanjem i snimanjem na licu mjesta. Nažalost, ograničena brzina prijenosa podataka i siromašne mogućnosti VMS-a osudile su oblak na propast te je trebalo mnogo godina da se ponovno pojavi kao značajan igrač unutar videonadzora.

U razdoblju između 2012. i 2014. godine mnogi su rubno skladištenje (eng. edge storage) vidjeli kao veliku inovaciju u pohrani podataka. Rubna pohrana ili lokalna pohrana u videonadzoru omogućuje snimanje videozapisa izravno na SD karticu u kameri, koderu ili uređaju za mrežnu pohranu tj. NAS (eng. Network Attached Storage). Cilj rubne pohrane bio je zamijeniti uređaje za snimanje s pohranom i programskom podrškom postavljene unutar same IP kamere, što je zbog problema s pouzdanošću te neusporedivo jeftinijim cijenama snimača, posebice na kineskom tržištu, rezultiralo neostvarenom idejom. S druge strane, u tom razdoblju kamere postaju znatno bolje u rukovanju pri izazovnim uvjetima snimanja, posebice u slučajevima pojačane rasvjete i potpune tame. Kamere sa širokim dinamičkim rasponom ili WDR-om (eng. Wide Dynamic Range) više nisu bile ograničene ni skupe te su se loše performanse kamere uzrokovane slabim osvjetljenjem kudikamo smanjile. Jedna od najvećih promjena u posljednjih 10 godina bio je

porast „pametnih kodeka“ (eng. „Smart CODEC“). Prednost ovog kodeka u odnosu na manje pametne kodeke je dinamičko prilagođavanje kompresije i I-okvira (eng. Intra frame or I-frame) temeljenih na analizi scene. Ovi kodeci neovisni su o H.264 ili H.265 video kodiranju, ali su se pri uvođenju prvenstveno koristili sa H.264. Iako su pametni kodeci smanjili korist dodavanja H.265 isporukom uštede propusnosti pomoću H.264, do 2018. gotovi svi proizvođači izdavali su nove kamere koje podržavaju H.265. Za razliku od danas, između 2000. i 2010. godine zbog tvrdih diskova male memorije ili HDD (eng. Hard Disk Drive), slabije učinkovite kompresije, sve veće potražnje za HD rezolucijom te ukupnog troška pohranjivanje videozapisa bio je izazov. Kombinacijom H.264/H.265 kompresija i sve boljeg omjera pohrane i cijene tvrdog diska ostvaruje se skladištenje videozapisa s manje problema nego ikad. U razdoblju od 2008. do 2013. razlučivost slike se u učetverostručila u odnosu na SD, od 0.3 MP do 1.3 MP. Sada se kvaliteta razlučivosti sporije povećava s vremenom, u prosjeku od 3 do 6 MP, što je puno sporije nego u razdoblju između 2005. i 2015. Slikom 3.1. prikazana je postotna promjena korištenja određene razlučivosti s vremenom.



Slika 3.1. Postotna promjena [1]

Dok su danas kamere od 3-5 MP zastupljene na većini lokacija, upotreba kamera od 8+ MP još je uvijek u velikoj manjini. Štoviše, na tržištu ima vrlo malo 12 MP kamera i dok se spominju kamere s 8K (tj. 33 MP), takva kvaliteta videonadzorne kamere još je uvijek uglavnom konceptualna. Više od desetljeća IP je bio jedini praktičan način dostave MP/HD, ali početkom 2010. godine pojavio se analogni HD prenošen pomoću koaksijalnog kabela. Zamijenio je analogni SD postavši bitan u prodaji kompleta za kućnu upotrebu te niskog i srednjeg tržišta. Iako je analogni HD povećao maksimalnu razlučivost sve do 8 MP i dodao ograničenu snagu u odnosu na koaksijalni kabel, u posljednjih nekoliko godina usporilo se njegovo usvajanje u odnosu na IP. Tijekom 2019. godine dolazi do povećanja mladih poduzeća (eng. start-up) zbog utjecaja umjetne inteligencije i Cloud-

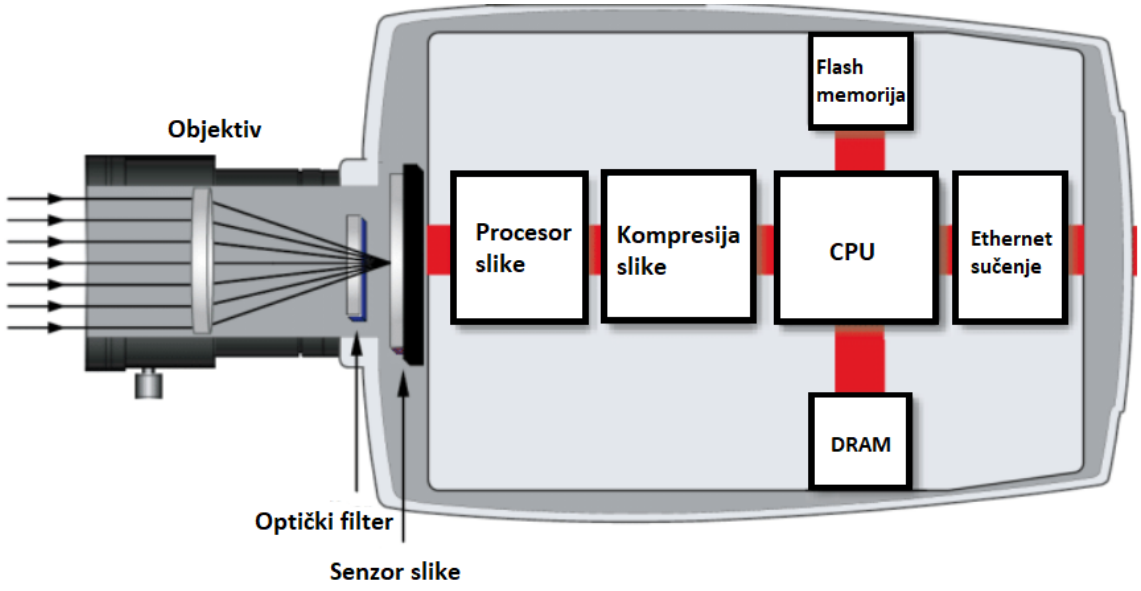
a. Dok su prethodne godine bile potaknute povećanjem razlučivosti i smanjenjem cijene, ovo razdoblje mnogo više oblikuje programska podrška za analizu videa koristeći duboko učenje (eng. deep learning) te upravljanje videom u oblaku. Iako i videoanalitika i oblak postoje već više od desetljeća, ovo povećanje startupa uzrokovano je globalnim poboljšanjem u analitici i zrelosti podržavajuće tehnologije oko oblaka, kao što su dostupnost propusnosti, infrastruktura oblaka, itd. Već iduće godine dolazi do novih promjena i problema uzrokovanih korona virusom. Neto prihod pao je tijekom godine jer su karantene ometale kupnju i ugradnju proizvoda. Također, nagli porast kupnje fotoaparata sredinom 2020. godine, ponajviše raznih oblika kamera za mjerenje temperature, rezultirao je neučinkovitim i namještenim uređajima. S druge strane, radi naglog porasta rada od kuće, sustavi u oblaku i daljinsko praćenje sustava poprimili su još više na važnosti, posebno zbog mogućnosti pristupa i upravljanja sustavom s bilo kojeg mjesta. Kako globalna ograničenja uzrokovana korona virusom nastavljaju popuštati tako se smiruje i tržište, a tehnologije i ponude u oblaku nastavljaju napredovati. Oblak i videoanalitika danas su široko rasprostranjeni, usvojeni kod najvećih i najvažnijih tvrtki svijeta, u kojima njihova upotreba iz temelja preoblikuje prodaju, postavljanje i funkciju videonadzora. [1]

4. OSNOVNE KOMPONENTE SUSTAVA VIDEONADZORA

Sustav videonadzora sastoji se od različitih elemenata koje rade zajedno kako bi omogućile nadzor, snimanje i analizu videozapisa određenog prostora. Osnovi elementi takvog sustava su IP kamere, mrežni snimač, mrežni preklopnik te mrežna infrastruktura. Bitno je razumjeti način na koji komponente u sustavu videonadzora rade te kako prilagoditi njihove postavke u svrhe postizanja željenog stupnja nadzora i sigurnosti.

4.1. IP kamere

IP video kamere sastoje se od nekoliko glavnih dijelova. Prvi je senzor slike, koji služi za pretvaranje svjetlosti koja pada na njega u digitalni signal. Druga važna komponenta je objektiv, koji usmjerava svjetlost na senzor i određuje karakteristike snimljenog materijala. Također, kamere koriste i algoritme kompresije videa za smanjenje veličine datoteka i olakšavanje prijenosa podataka preko mreže. Ugrađena ploča za obradu podataka obavlja funkcije poput obrade slike, kompresije videa i upravljanja mrežom. Ethernet sučelje omogućuje povezivanje kamere s IP mrežom za prijenos videozapisa i daljinsko upravljanje. Na kraju, kućište štiti unutarnje komponente od vanjskih utjecanja te je najčešće otporno na vremenske uvjete. Jedan od primjera IP video kamere prikazan je slikom 4.1., gdje se navedene značajke i funkcionalnosti mogu razlikovati ovisno o modelu i proizvođaču kamere.



Slika 4.1. Dijelovi kamere [3]

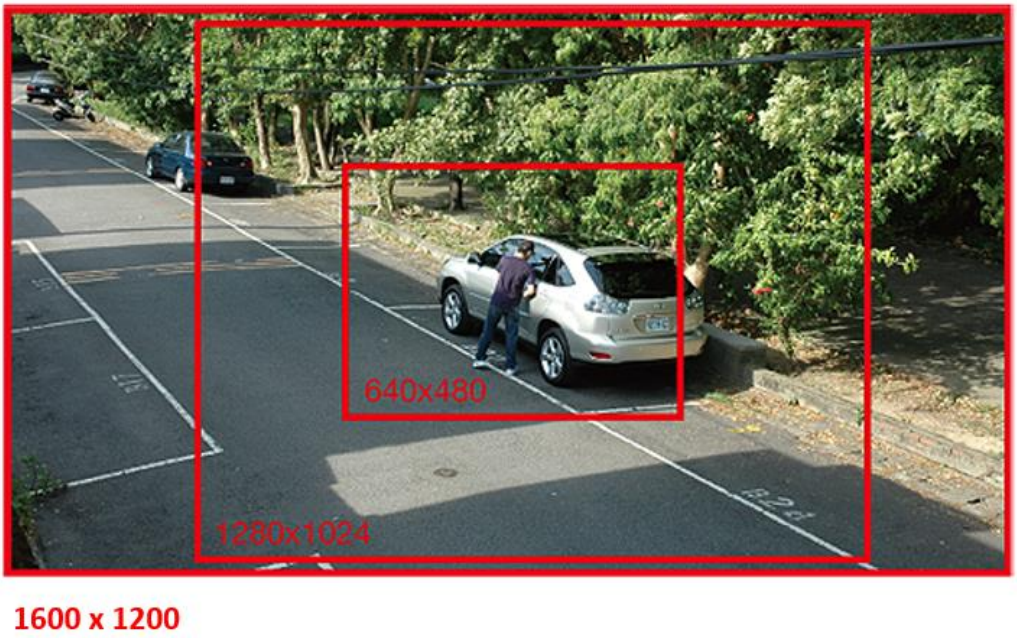
4.1.1. Senzor slike

IP kamere koriste senzore slike za pretvorbu svjetlosti u električne signale. Dvije najčešće korištene tehnologije su CCD (eng. Charge-Coupled Device) i CMOS (eng. Complementary Metal-Oxide-Semiconductor). CCD senzori godinama su bili najčešće korišteni senzori u industriji. Oni koriste kondenzatore za zapis svjetlosnih informacija te su poznati po visokoj kvaliteti slike i dobrim performansama u uvjetima slabog osvjetljenja. S druge strane, CMOS senzori koriste mrežu piksela s vlastitim tranzistorima te iz tog razloga ostvaruju brži rad i manju potrošnju energije. Usporedba CCD i CMOS senzora prikazana je tablicom 4.1.

Tablica 4.1. Usporedba CCD i CMOS senzora slike [4]

Karakteristike	CCD	CMOS
Osjetljivost	Visoka	Niska
Šum	Niski	Umjereni
Zatvarač (eng. Shutter)	Globalni	Rolo zatvarač
Potrošnja energije	Visoka	Niska
Signal piksela	Elektroni	Napon
Izlaz senzora	Analogni	Digitalni
Složenost sustava	Visoka	Niska

Osim vrste senzora slike, s godinama se mijenjala i njihova razlučivost. Razlučivost senzora odnosi se na broj piksela koje senzor može snimiti čime veća razlučivost rezultira preglednijom slikom. Osnovna razlučivost od 640x480 piksela koja pruža prihvatljivu kvalitetu slike pri manje zahtjevnim primjenama je VGA (eng. Video Graphics Array). Dolaskom digitalnih video kamera pojavljuje se HD i Full HD (eng. High Definition) razlučivost senzora. Takve kamere obično koriste senzore s 1280x720 piksela (720p) i 1920x1080 piksela (1080i ili 1080p) te su trenutno najrasprostranjenije na tržištu. Razlika u vidljivosti scene ovisno o razlučivosti prikazano je slikom 4.2.



Slika 4.2. Različite rezolucije slike [5]

Sve popularniji postaju 2K i 4K senzori korišteni za identifikaciju lica, detekciju kretnje ili prebrojavanje objekata kao i prepoznavanje registarskih oznaka vozila. Velika razlučivost slike obično zahtijeva više resursa za pohranu i obradu podataka čime se troškovi znatno povećavaju. Tehnologija senzora slike i njihove karakteristike stalno se razvijaju čime nastaju različite varijante i poboljšanja. Prilikom odabira IP kamere bitno je razmotriti tip senzora slike, njegovu rezoluciju i druge specifikacije koje utječu na kvalitetu snimke koju kamera može snimiti. [6]

4.1.2. Objektiv

Objektiv je dio kamere koji ima važnu ulogu u procesu snimanja. Služi za prikupljanje i usmjeravanje svjetlosti prema senzoru kamere, čime omogućuje stvaranje slike. Glavni dijelovi objektiva su leće, apertura (otvor blende) i iris. Postoje različite vrste objektiva, a svaka od njih ima svoje karakteristike koje utječu na kvalitetu slike i mogućnosti snimanja. Primjerice, žarišna duljina određuje kut gledanja i veličinu slike, dok veličina otvora aperture utječe na svjetlinu i dubinsku oštrinu slike. Važno je odabrati optimalni objektiv ovisno o vrsti snimanja koja se želi ostvariti kao i osobnim potrebama i željama.

Slika 4.3. Objektiv video kamere [7]

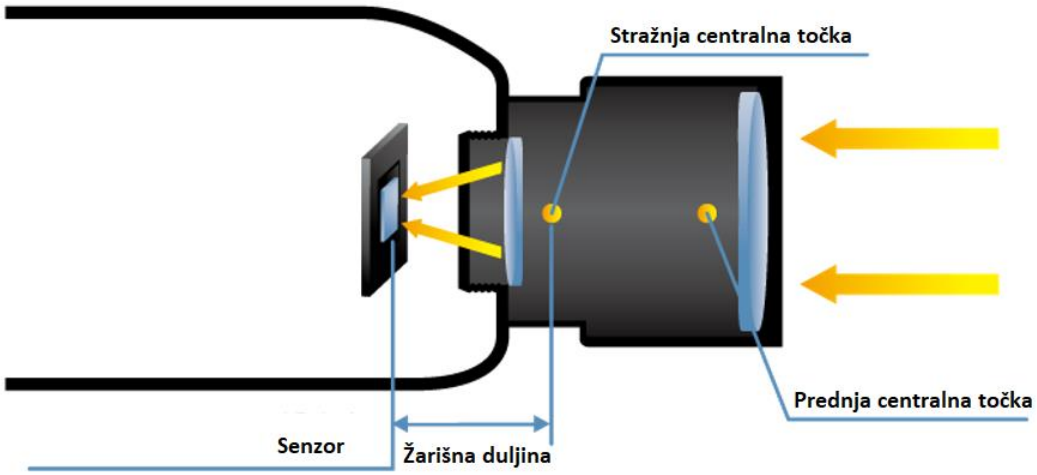
Apertura u video kameri je otvor u objektivu koji regulira količinu svjetlosti koja ulazi u kameru. Velika apertura (širi otvor) dopušta više svjetlosti da prodre u objektiv i stigne do senzora, što čini sliku svjetlijom prikazano na lijevo strani slike 4.4. S druge strane, mala apertura (uži otvor) dopušta manje svjetlosti da prodre u objektiv, što čini sliku tamnijom prikazano na desnoj strani slike 4.4.

Slika 4.4. Ovisnost kvalitete slike o aperturi [8]

Osim utjecaja na osvjetljenje, apertura također ima veliki utjecaj na dubinsku oštrinu slike. Što je apertura šira, to je manji dio slike koji će biti oštar, dok će ostatak biti zamagljen. S druge strane, manja apertura ima veću dubinsku oštrinu, što znači da će veći dio slike biti oštar. Dubinska oštrina slike ima veliki utjecaj na percepciju dubine i trodimenzionalnosti slike. [9]

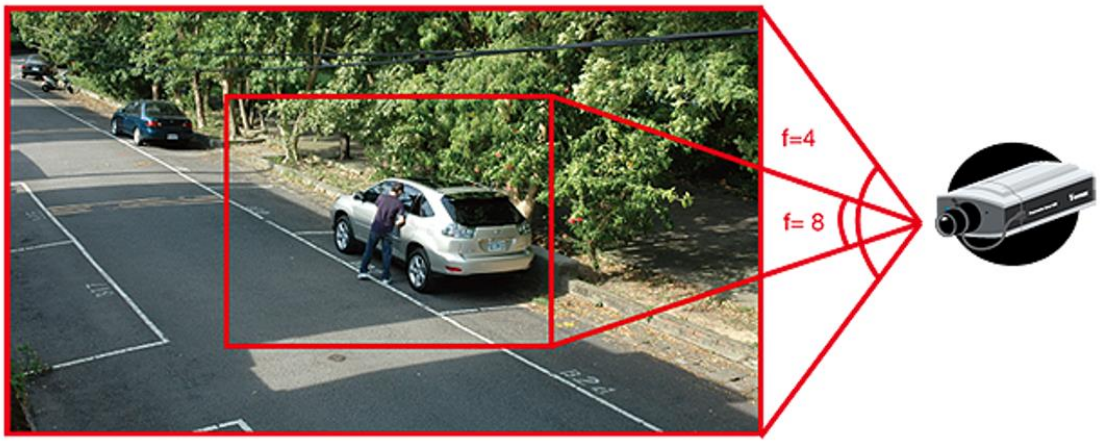
4.1.3. Karakteristike objektiva

Karakteristike objektiva od velike su važnosti u oblikovanju i kvaliteti slike nastale iz promatrane scene. Najznačajnije karakteristike su: žarišna duljina, iris, f-broj, dubina polja i defrakcija. Žarišna duljina kod video kamera označava udaljenost između leće objektiva i točke na kojoj se svjetlosne zrake susreću i formiraju oštru sliku, prikazano na slici 4.5.



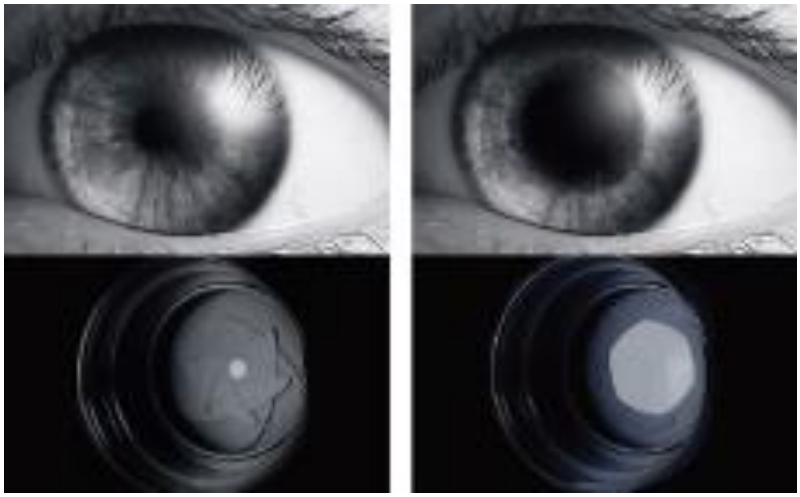
Slika 4.5. Unutrašnjost objektiva i kamere [10]

Ona ima važnu ulogu u određivanju kuta gledanja, dubinske oštrine i sposobnosti fokusiranja objekta na kameri. Osim toga, žarišna duljina utječe na udaljenost na kojoj kamera može fokusirati objekt. Objektivi s kraćom žarišnom duljinom omogućuju širi kut gledanja, dok objektivi s dužom žarišnom duljinom imaju uži kut gledanja i bolju kontrolu dubinske oštrine, kao što je vidljivo na slici 4.6.



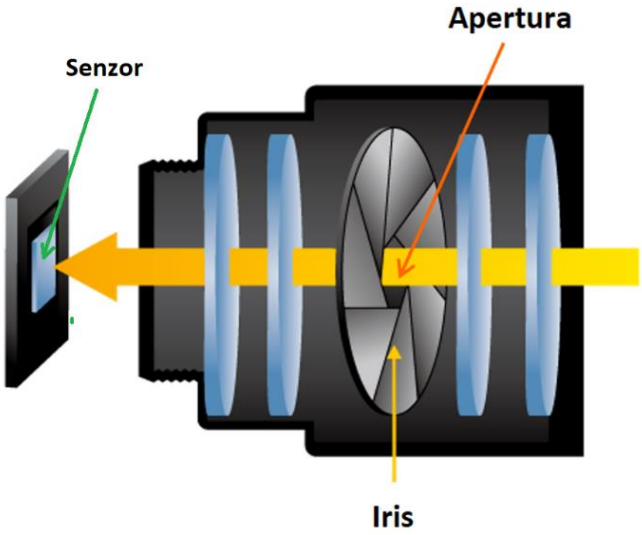
Slika 4.6. Odnos žarišne duljine i kuta gledanja [11]

Kraća žarišna duljina osigurava šire pokrivanje, dok se s dužom žarišnom duljinom ostvaruje uže pokrivanje scene. Elektronički sustav koji se nalazi unutar objektiva i služi za kontrolu količine svjetlosti koja ulazi u njega zove se iris. Funkcija irisa u kamerama inspirirana je irisom u ljudskom oku (slika 4.7.).



Slika 4.7. Sličnost ljudskog oka i irisa [12]

Za prilagodbu na količinu i intenzitet svjetlosti iris u ljudskom oku koristi mišićne kontrakcije, dok iris u kamerama koristi mehanički sustav aperture, tj. niz pokretnih krilaca koji se otvaraju i zatvaraju kako bi se regulirala veličina otvora aperture. Na slici 4.8. prikazan je prolaz svjetlosti kroz iris i aperturu te dolazak na senzor.



Slika 4.8. Razlika irisa i aperture [13]

Osim što kontrolira količinu svjetlosti, iris igra važnu ulogu u regulaciji dubinske oštrine slike. Pomoću regulacije otvora aperture, može se postići veća ili manja dubinska oštrina, ovisno o željenom efektu. Širi otvor blende uzrokuje pliću dubinsku oštrinu, pri čemu je manji dio slike oštar, a ostatak je zamagljen. S druge strane, uži otvor ima veću dubinsku oštrinu i omogućava fokusiranje više dijelova slike. Iris se može kontrolirati na više načina:

1. Ručno – koristi se u slučaju nepromjenjive količine svjetlosti, podešavanje se vrši pomoću prstena na objektivu.
2. Automatsko – razlikuju se:
    a. DC iris – upravljanje DC strujnim krugom,
    b. Video iris - video signal prenosi se na upravljački krug objektiva te konvertira u struju potrebnu za upravljanje motorima irisa i
    c. Precizni iris ili P-iris – koristi motor koji ostvaruje preciznu daljinsku kontrolu otvora aperture.
3. Fiksni iris – ne može se podešavati otvor irisa.

Automatsko upravljanje irisom koristi senzor svjetla na kameri kako bi automatski prilagodio veličinu aperture prema uvjetima osvjetljenja, dok se ručno upravljanje irisom koristi za fino ugađanje kada je potrebna veća preciznost u kontroli osvjetljenja i dubinske oštrine slike. P-iris tehnologija je koja se sastoji se od posebnog elektromagnetskog mehanizma koji može kontrolirati otvor aperture objektiva na način koji je mnogo precizniji od tradicionalnih mehaničkih irisa, kao što je vidljivo na slici 4.9.

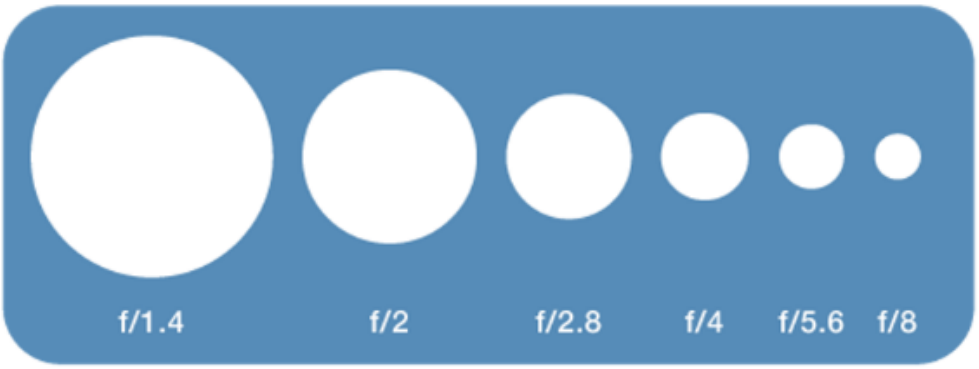
Slika 4.9. Usporedba DC irisa i P-irisa [14]

P-iris obično se koristi u industrijskim i profesionalnim video kamerama, gdje je precizna kontrola otvora aperture ključna za postizanje visoke kvalitete slike. Pri korištenju P-irisa, kamera može automatski podešavati otvor aperture na temelju promjena u osvjetljenju, što omogućuje postizanje optimalne ekspozicije. Također, ovu tehnologiju moguće je koristiti i u kombinaciji s drugim tehnologijama, poput automatskog fokusa u svrhe postizanja još bolje kvalitete slike i performansi video kamere. [15]

F-broj predstavlja omjer između veličine otvora aperture i žarišne duljine objektiva kod video kamera, prikazano formulom:

$$F - broj = \frac{žarišna\ duljina}{promjer\ objektiva(apertura)}\ . \qquad (4.1)$$

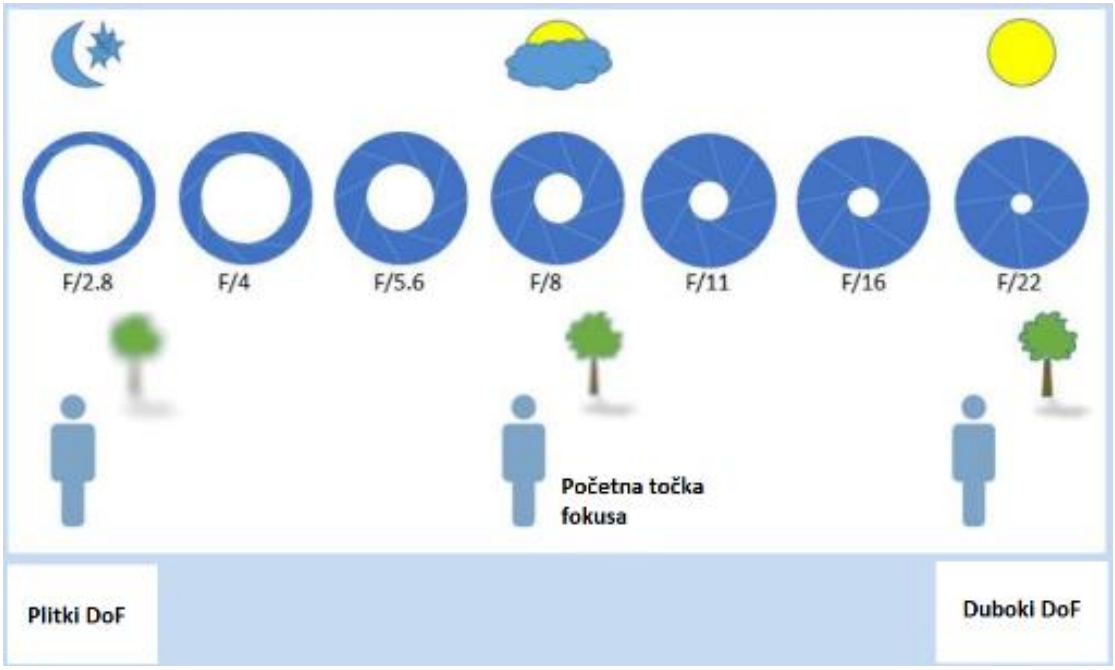
Ova vrijednost označava se kao razlomak (npr. f/2.8 ili f/4), gdje niži f-brojevi predstavljaju širi otvor aperture što omogućava prolazak više svjetlosti kroz objektiv i samim time svjetlijom slikom. Međutim, niži f-brojevi imaju manju dubinsku oštrinu, što uključuje manji dio slike koji je u fokusu. Iz tog razloga, niži f-brojevi korisni su u situacijama slabijeg osvjetljenja ili pri izdvajanju pojedinog objekta iz pozadine slike. S druge strane, viši f-brojevi znače uži otvor aperture što rezultira tamnijom slikom. Na slici 4.10. prikazana je ovisnost otvora aperture o f-broju.



Slika 4.10. Ovisnost f-broja o otvoru aperture [16]

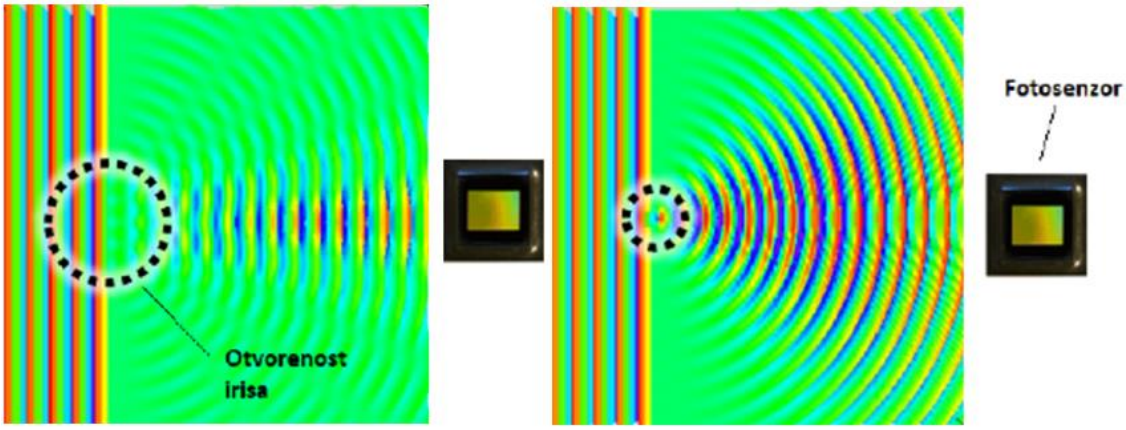
Također, viši f-brojevi imaju veću dubinsku oštrinu što uzrokuje fokusiranje većeg dijela slike čime su viši f-brojevi korisni u situacijama kada se želi postići veća dubinska oštrina, poput snimanja krajolika ili grupe ljudi. F-broj moguće je podešavati ručno ili automatski, ovisno o potrebama snimanja. Ručno podešavanje f-broja koristi se kada je potrebna preciznija kontrola nad svjetlosnim uvjetima i dubinskom oštrinom slike, dok se automatsko podešavanje koristi za brze promjene fokusa ili dubinske oštrine. [17]

Dubina polja ili DoF (eng. Depth of field) u video kameri označava područje ispred i iza točke fokusa koje će biti oštro na snimci, dok će se ostatak scene prikazati mutno. Dubina polja ovisi o žarišnoj duljini objektiva, otvoru aperture i udaljenosti između objekta i kamere. Što je žarišna duljina objektiva veća, a otvor aperture manji, dubina polja će biti veća, a ako je žarišna duljina manja, a otvor aperture veći, dubina polja će biti manja. Tijekom svijetlog dana, apertura se zatvara stvarajući duboki DoF te su tada svi objekti, bliski i daleki, u fokusu unutar slike (slika 4.11.). [18]



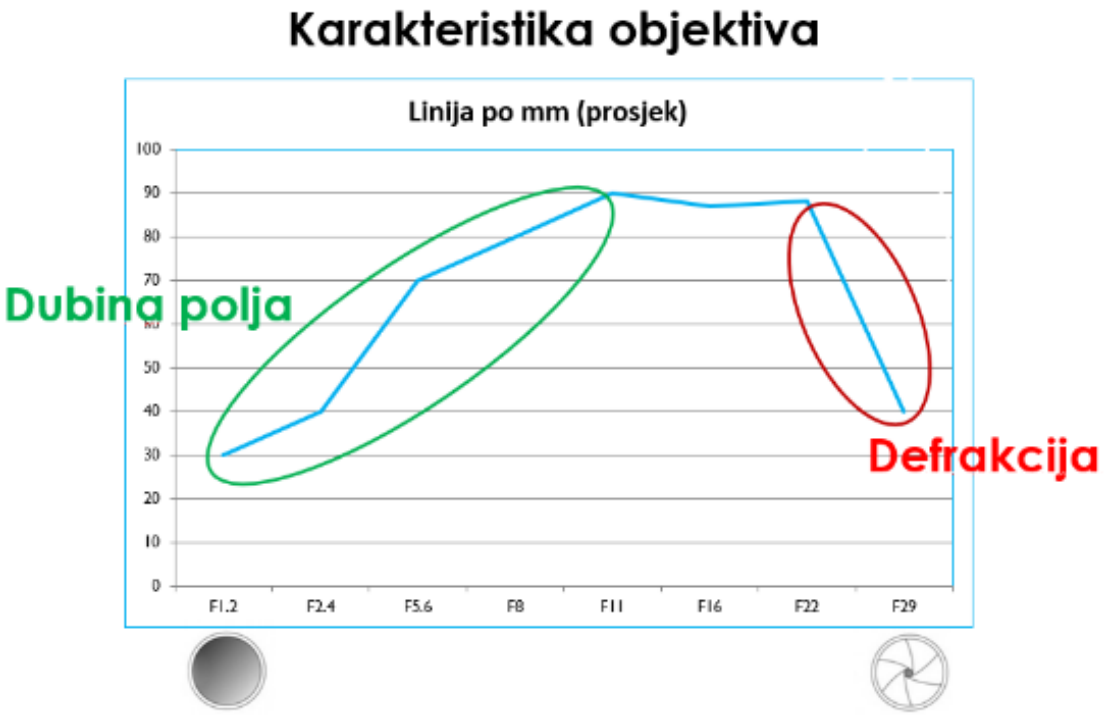
Slika 4.11. Vidljivost slike ovisna o dubini polja [19]

Dubina polja važna je jer utječe na izgled snimke i koristi se za postizanje određenog efekta, ovisno o tome što se snima. Pojava savijanja svjetlost pri prolasku kroz optička sredstva, poput objektiva na video kameri, nazive se defrakcija. Kod video kamera, defrakcija se obično pojavljuje kada svjetlost prolazi kroz objektiv i fokusira se na senzor kamere. Savijanje i iskrivljivanje svjetlosnih zraka rezultira izobličenjem slike i smanjenja njene kvalitete. Da bi se smanjio utjecaj defrakcije, proizvođači kamera koriste posebne optičke elemente u objektivu, poput specijalnih stakala ili premaza, koji pomažu u smanjenju savijanja svjetlosti. Također, važno je imati na umu da se defrakcija može pojaviti u različitim uvjetima osvjetljenja i ovisi o karakteristikama objektiva kamere. Pri jakim osvjetljenjem te samim time jako malom otvoru aperture dolazi do smanjenja oštrine, tj. defrakcije svjetlosti, što je prikazano na slici 4.12.



Slika 4.12. Ovisnost defrakcije svjetlosti o otvorenosti irisa [20]

U konačnici, defrakcija svjetlosti može utjecati na kvalitetu slike video kamere, stoga je važno uzeti u obzir ovaj čimbenik pri odabiru objektiva i snimanju videozapisa. Na slici 4.13. prikazane su značajke leće objektiva. Vidljivo je da kvaliteta slike opada pri širem irisu (manjem F broju) zbog kratke i ograničene dubine polja kao i u slučaju manjeg irisa (većeg f-broja) pri pojavi defrakcije svjetlosti.



Slika 4.13. Karakteristike leće objektiva [21]

Optimalna kvaliteta slike postignuta je u srednjem rasponu f-broja koju je u praksi korištenjem fiksnog ili DC irisa teško zadržati. Razlog tome je nedostatak informacije o točnom položaju irisa te isključivo mogućnost otvaranja i zatvaranja irisa ovisno o količini svjetlosti. U tom slučaju potreban je objektiv čija funkcija omogućava precizno upravljanje irisom – Precizni iris. [21]

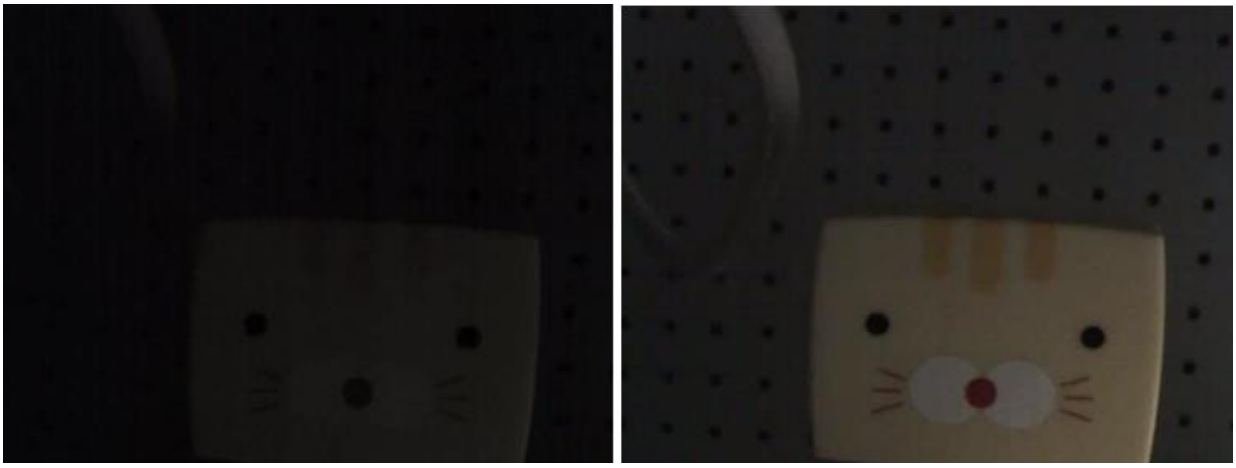
4.1.4. Karakteristike kamere

Karakteristike kamere obuhvaćaju niz tehničkih značajki i specifikacija koje određuju funkcionalnost i sposobnost snimanja. Najbitnije značajke su ekspozicija i brzina zatvarača, dinamički raspon, ravnoteža bijele boje, osjetljivost i dan/noć način rada. Ekspozicija predstavlja izlaganje fotosenzora svjetlosti, tj. trajanje otvorenosti električnog zatvarača (eng. Electronic shutter). To vrijeme naziva se i brzina zatvarača (eng. shutter speed) te može biti vrlo kratko, od nekoliko tisućinki sekunde sve do nekoliko minuta, ovisno o postavkama kamere i uvjetima snimanja. Brzina shutter-a određuje kolika količina svjetlosti će doći na senzor kamere, što utječe

na količinu detalja i kvalitetu slike. Kraće vrijeme ekspozicije koristi se u situacijama kada se snima brza akcija ili se pokušava zamrznuti pokret, dok se duže vrijeme ekspozicije koristi u uvjetima slabog osvjetljenja kako bi se snimila svijetla i detaljna slika. [22] Na kvalitetu slike utječu i dinamika promatranog objekta kao i njegovo okruženje. Ako se za primjer uzme snimanje osoba u kretnji na otvorenom prostoru (veće osvjetljenje), pri maloj brzini shutter-a kretnje će biti iskrivljene i zamagljene, a slika presvijetla te je u tom slučaju potrebno ostvariti manje vrijeme ekspozicije, kao što je vidljivo slike 4.14.

Slika 4.14. Ovisnost brzine shutter-a o dinamici scene [23]

S druge strane, prikazano slikom 4.15., promatranjem nepomičnog predmeta u uvjetima slabijeg osvjetljenja, uslijed male ekspozicije dobiti će se zamračena slika te je iz tog razloga potrebno imati veću brzinu shutter-a.

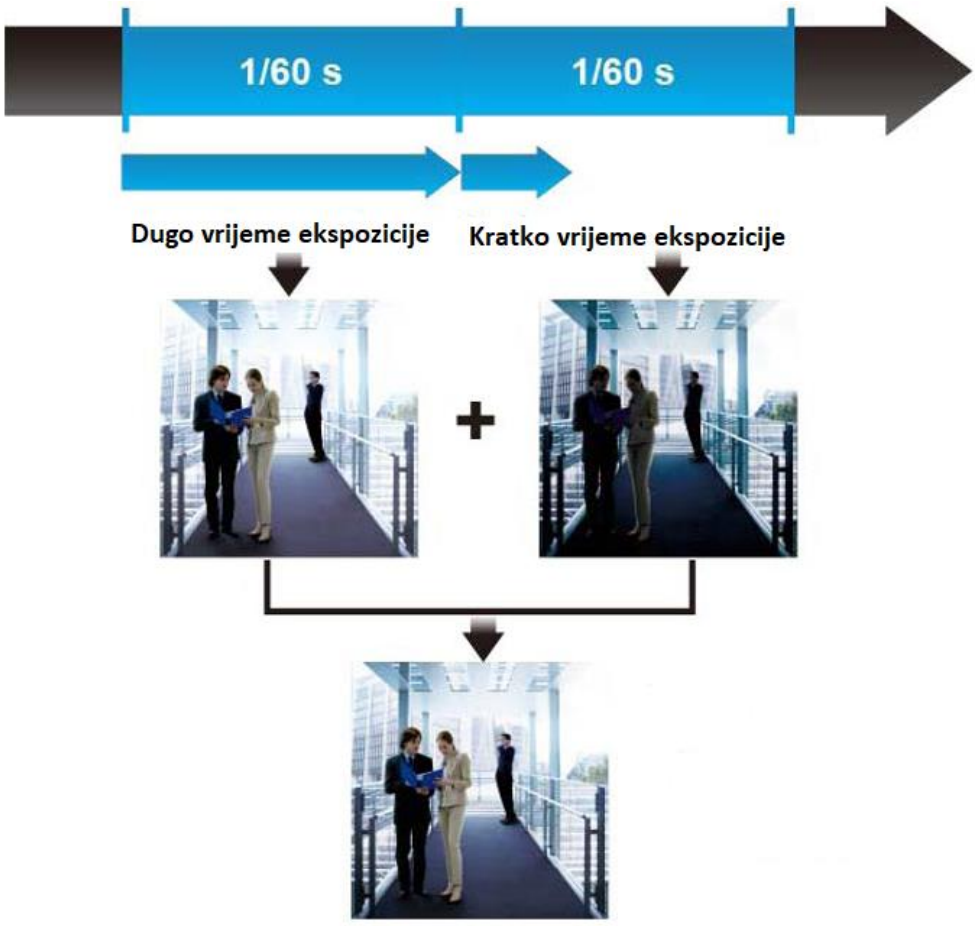


Slika 4.15. Ovisnost brzine shutter-a o dinamici scene [24]

Isto tako, moguće je upravljati pojačanjem (eng. Gain) signala čime je u prethodno navedenom slučaju moguće ostvariti veću kvalitetu slike. Veliko pojačanje rezultira vidljivijom slikom, ali i pojavom šuma koji će imati negativan utjecaj na njenu kvalitetu. Zbog proporcionalnog odnosa

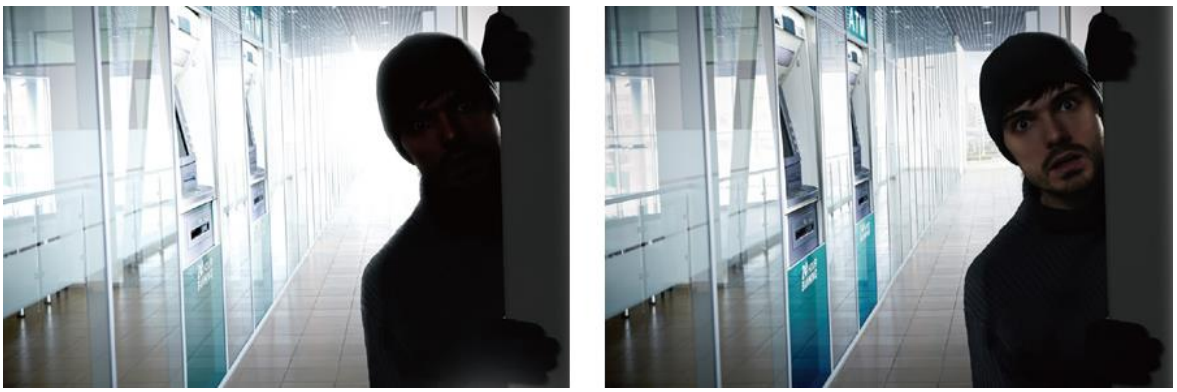
pojačanja i šuma potrebno je pravilno upravljati tim faktorom kako bi se dobila što kvalitetnija slika.

Široki dinamički raspon ili WDR (eng. Wide Dynamic Range) tehnologija je koja kod kamera omogućuje jednostavnije upravljanje širokim spektrom osvjetljenja u promatranoj sceni. WDR pomaže u očuvanju detalja i izbjegavanju prekomjernog osvjetljenja ili potamnjenja u scenama s visokim kontrastom svijetlih i tamnih područja kombiniranjem dvije slike s različitom ekspozicijom. Na slici 4.16. prikazan je princip rada WDR-a gdje se jedna visokokontrastna slika stvara kombiniranjem dva kadra pomoću naprednog procesora slike.



Slika 4.16. Princip rada WDR-a [25]

Ova tehnologija posebno je korisna u situacijama s jakim izvorom svjetlosti, kao što su ulična rasvjeta, prozori ili ulazna vrata gdje bi se inače izgubili detalji slike (slika 4.17.).



Slika 4.17. WDR pri jakom izvoru svjetlosti [26]

Ravnoteža bijele boje ili skraćeno WB („White balance“) postupak je prilagođavanja boje snimanog sadržaja uklanjanjem nerealnih nijansi boja nastale uslijed određenih vrsta osvjetljenja kako bi se postigla točna raspodjela boja u skladu s referentnom bijelom bojom. Primjeri raznih vrsta osvjetljenja scene prikazani su tablicom 4.2.

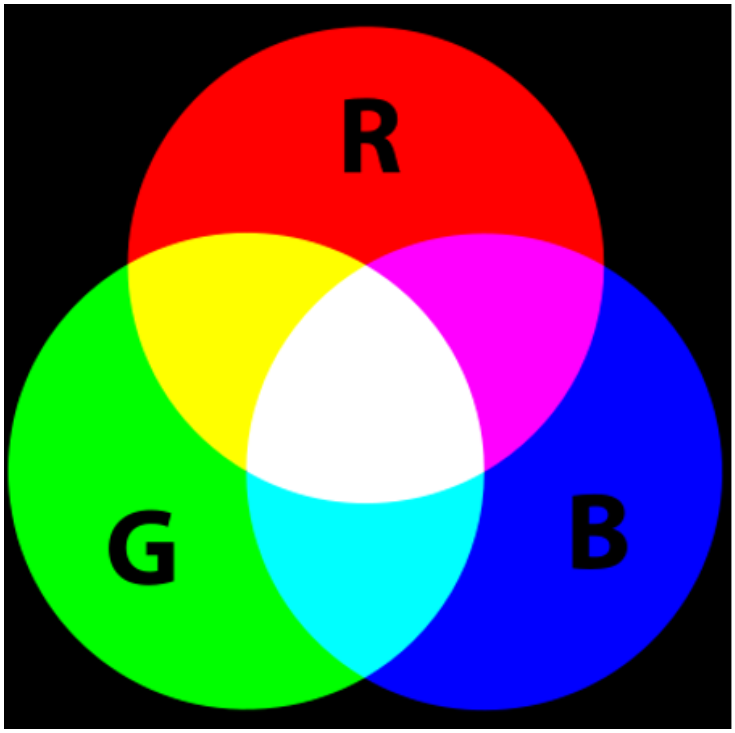
Tablica 4.2. Temperature boja u kelvinima [27]

Vrsta svjetla	Temperatura boje [K]
Svjetlo svijeće	1500
Svjetlo u kućanstvima	3000
Izlazak sunca	3500
Direktno sunce	5500
Sunčano vrijeme	6000
Oblačno vrijeme	7000
Plavo nebo	8000

Uslijed postavljanja kamere na automatski način rada bijele boje ili AWB (eng. Auto White Balance), senzor kamere analizira osvjetljenje scene i prilagođava postavke bijele boje kako bi neutralizirao boje nastale iz pripadajućeg osvjetljenja. Kao što je vidljivo sa slike 4.18., lijevo je prikazan objekt prije, a desno netom nakon korištenja funkcije AWB.

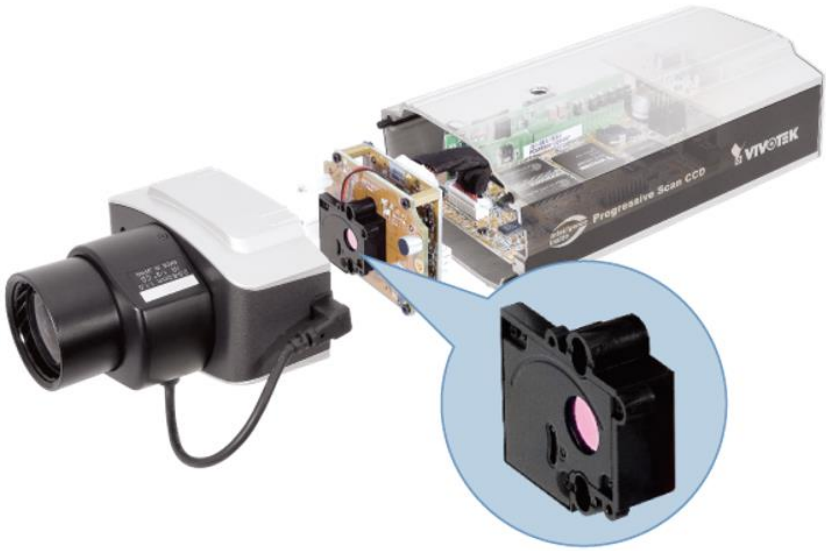
Slika 4.18. Utjecaj AWB-a na sliku [28]

Također, prilagođavanje boje slike može se ostvariti i ručno miješanjem crvene, zelene i plave boje (eng. RGB). RGB model kombinira intenzitete crvene, zelene i plave svjetlosti kako bi stvorio širok spektar boja, kao što je prikazano na slici 4.19.



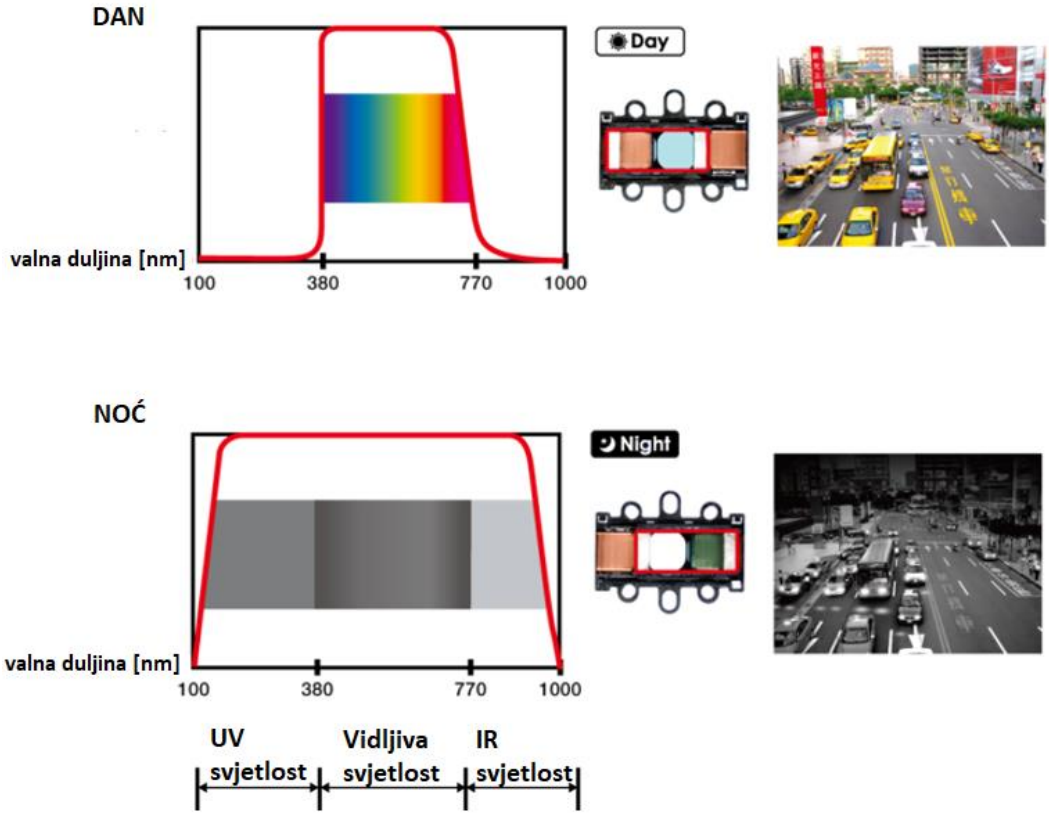
Slika 4.19. RGB model [29]

Kada su sve tri boje kombinirane s punim intenzitetom dolazi do stvaranja bijele boje dok odsutnost svih boja rezultira crnom bojom. Dan/Noć način rada (eng. Day/Night mode) odnosi se na sposobnost kamere da automatski prilagodi svoje postavke kako bi se omogućile optimalne snimke u različitim uvjetima dnevnih i noćnih osvjetljenja. Pri noćnom radu obično se uključuje infracrveni osvjetljivač (eng. IR illuminator), tj. ugrađene infracrvene LED diode koje u uvjetima slabog osvjetljenja kameri dodatno osvjetljavaju scenu. Filter koji u dnevnom načinu rada sprječava utjecaj infracrvenih LED dioda zove se „IR cut filter“ (slika 4.20.).



Slika 4.20. IR filter [30]

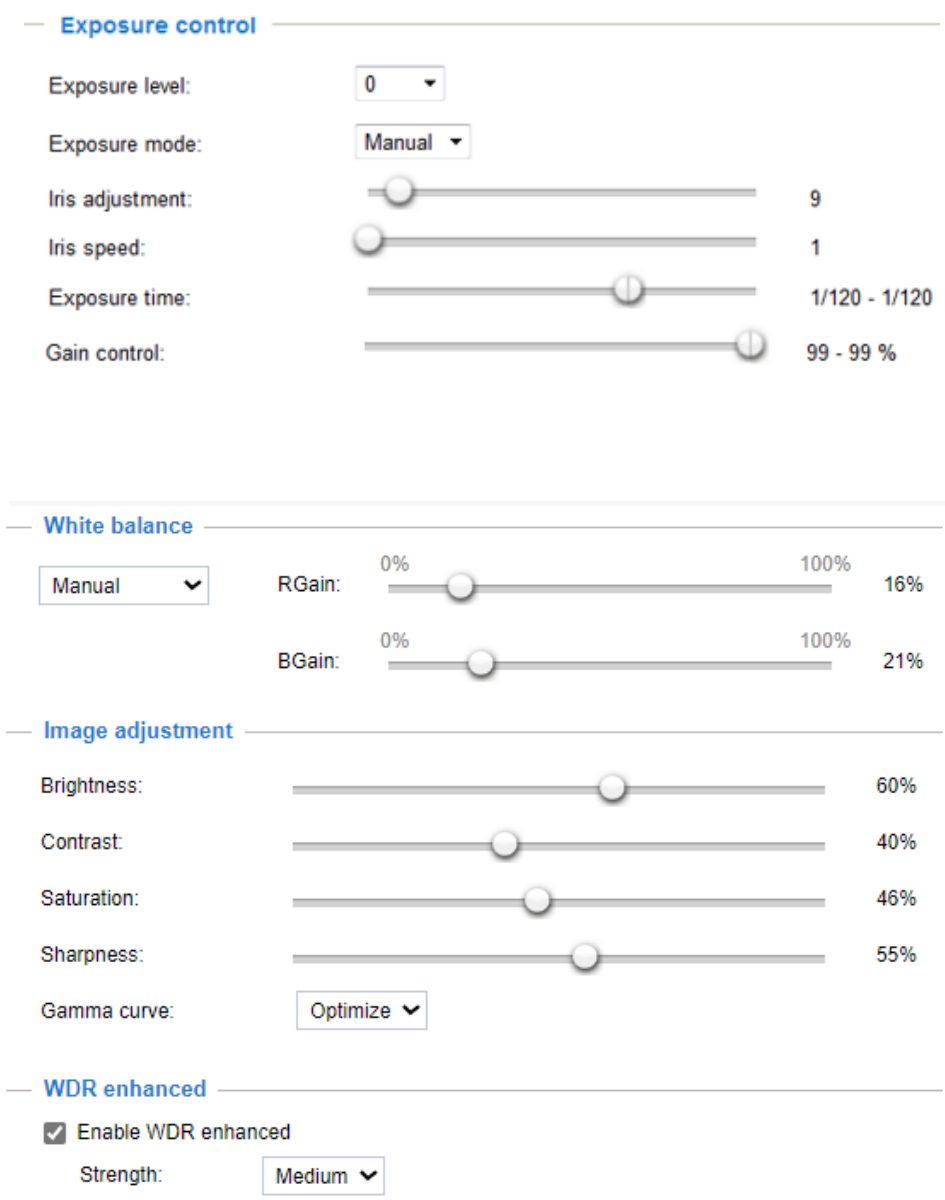
To je mehanički zatvarač upravljan motorom ili elektromagnetom koji se postavlja između objektiva i senzora slike. Kao što je vidljivo sa slike 4.21., u dnevnom režimu rada kamere, kada je potrebno propuštati samo vidljivu svjetlost u rasponu valne duljine od 380 do 770 nanometara, filter je postavljen, dok se u noćnim uvjetima propušta puni frekvencijski raspon svjetlosti kako bi se ostvarila što moguće veća vidljivost kamere.



Slika 4.21. Day/Night režim rada [31]

Osjetljivost kamere odnosi se na sposobnost hvatanja svjetla i stvaranje slike, posebno u uvjetima različitih razina osvjetljenja. To je mjera koliko dobro kamera može reagirati na svjetlo i generirati kvalitetan slikovni zapis, čak i u uvjetima slabog svjetla. Veća osjetljivost omogućuje kameri bilježiti više detalja čak i u slučaju slabijeg osvjetljenja, dok manja osjetljivost rezultira tamnim ili zrnastim slikama u istim uvjetima. Osjetljivost kamere iskazuje se u luksima pri određenom f-broju objektiva. U noćnom režimu (crno-bijelo) rada osjetljivost je bolja nego u dnevnom režimu (u boji) dok je pri infracrvenom osvjetljenju iznos osjetljivosti jednaka nuli što rezultira vidljivom slikom i u slučaju potpunog mraka. [32]

U donedavno korištenim analognim kamerama na većinu se navedenih funkcija moglo utjecati isključivo na samoj kameri. Takvo umjeravanje iziskivalo je dulje vrijeme i veće iskustvo u odnosu na programsko umjeravanje korišteno u današnjim videonadzornim sustavima. Na slici 4.22. prikazano je Vivotek programsko sučelje za umjeravanje IP kamere korištenjem internetskog preglednika.



Slika 4.22. Postavke kamera u Vivotek internet pregledniku

Prilagodbom do sad navedenih čimbenika uvelike se utječe na kvalitetu promatrane scene te ih je iz tog razloga nužno razumjeti i naučiti umjeravati.

4.1.5. Vrste IP kamera

U sustavu videonadzora koriste se različite vrste kamera, svaka sa svojim specifičnim karakteristikama i namjenom. U prošlosti su kamere za videonadzor većinom bile kvadratnog oblika (eng. box camera) na koju se naknadno stavljao objektiv, gdje se za postavljanje na otvorenom mjestu koristilo vanjsko kućište. Danas su takve kamere i dalje u upotrebi, najčešće kada je potreban objektiv većeg raspona žarišne duljine ili zoom objektiv te u slučajevima kada kućište kamere treba biti u specijalnoj izvedbi (inox kućište ili kućište s vodenim hlađenjem).

Međutim, u svakodnevnim aplikacijama uglavnom se koriste kompaktne kamere koje uključuju i objektiv. Za vanjsku upotrebu većinom su to „bullet“ kamere, dok su za unutarnje instalacije pogodnije kupolaste „dome“ kamere. Primjeri navedenih vrsta kamera marke Vivotek dani su slikom 4.23.

Slika 4.23. Vrste IP kamera [33]

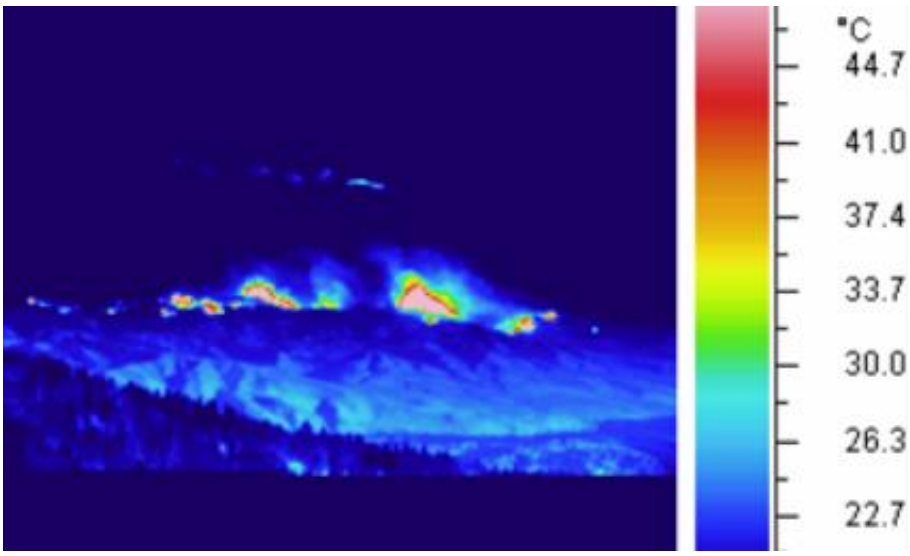
IP kamere također dolaze i u specijalnim izvedbama prilagođene specifičnim potrebama u određenim situacijama. U slučaju nadzora većeg prostora bez mrtvih kutova korisna je „fisheye“ stropna kamera koja ima mogućnost snimanja okoline od 360 stupnjeva, dok se za snimanje vidnog polja od 180 stupnjeva koristi panoramska kamera, prikazane na slici 4.24.

Slika 4.24. „Fisheye“ i panoramska kamera [34]

Kamera koja ima sposobnost daljinskog upravljanja pozicijom i zumiranjem objektiva zove se PTZ (eng. Pan-Tilt-Zoom) kamera, a koristi se u nadzoru prometa, stadiona, trgova itd. Takve pokretne kamere su znatno skuplje i većih dimenzija od prijašnje navedenih zato što osim kamere sadrže i motor koji ostvaruje vodoravnu i okomitu kretnju. Najčešća izvedba PTZ kamere je u obliku pokretne dome kamere, iako su prisutne i izvedbe s kućištem u koje se postavlja box kamera, kao što je prikazano slikom 4.25.

Slika 4.25. Vrste PTZ kamera [35]

Tipovi kamera koje su korisne za detektiranje topline koju promatrani objekti emitiraju naziva se termalna kamera. Ovakva kamera omogućava vizualizaciju razlike u temperaturi između različitih objekta i okoline te su korisne u situacijama smanjene vidljivosti, vidljivo sa slike (4.26.).



Slika 4.26. Primjer prikaza scene termalne kamere [36]

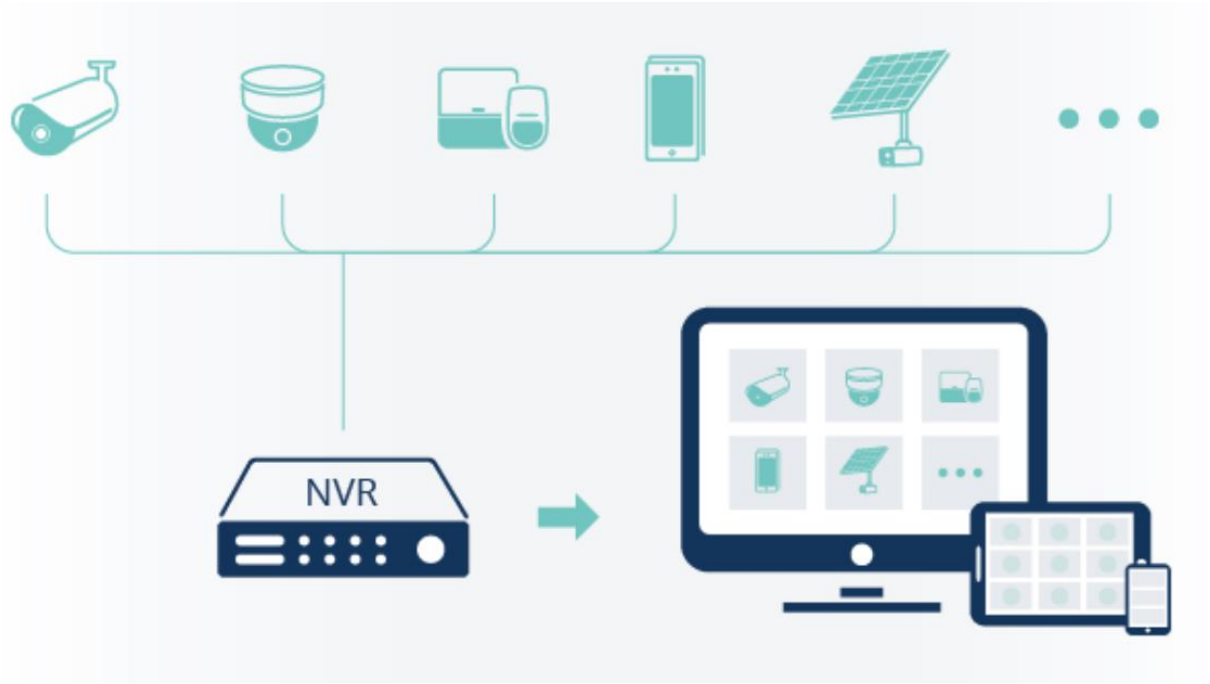
U svrhe prikrivenog nadzora kao što su bankomati, koriste se male kamere s „pinhole“ ili „fisheye“ objektivom ugrađene u svakodnevne predmete ili okoline. Takve kamere mogu biti kompaktne ili izvedene s odvojenom elektronikom koja je kabelom spojena s glavom kamere i objektivom, tzv. split tip kamere (slika 4.27.).

Slika 4.27. „Pinhole“ kamere [37]

Svaki tip kamere ima svoje prednosti i nedostatke te je nužno odabrati onu koja najbolje odgovara potrebama korisnika i zadanom okruženju.

4.2. Mrežni video snimač

U sustavu videonadzora, mrežni video snimač ili NVR (eng. Network Video Recorder) je uređaj koji se koristi za pohranu, pregled i upravljanje snimkama IP kamera. Na slici 4.28. prikazan je sustav videonadzora sa snimačem kao centralnim uređajem te načinima prikaza snimane scene.



Slika 4.28. Sustav videonadzora sa snimačem [38]

Ovisno o modelu i proizvođaču, NVR može imati različite karakteristike i značajke, uključujući podršku ovisno o broju kamera, razlučivost i snimanje u stvarnom vremenu. Glavni dijelovi mrežnog snimača uključuju unutarnju pohranu, CPU, mrežne portove, video ulaze i HDMI/VGA izlaze te operacijski sustav i programske aplikacije. Mrežni snimači najčešće nemaju standardni operativni sustav već koriste OS niže razine. Unutarnja pohrana snimača obično je u obliku tvrdog diska ili SSD-a (eng. Solid State Disk). Procesor služi za obradu, komprimiranje i enkripciju video snimki, a mrežni portovi služe za povezivanje IP kamera i lokalne mreže s NVR-om, gdje neki mrežni snimači imaju i PoE portove za napajanje kamera preko Ethernet kabela. Video izlazi putem HDMI/VGA priključaka omogućuju prikaz sadržaja video snimki na monitoru, dok se za daljinsko upravljanje i pristup putem interneta koriste web preglednik ili klijentska aplikacija. Također, NVR omogućuje podešavanje postavki snimanja, vremenske rasporede i ograničeni pristup snimki. [39]

Jedan od najbitnijih izračuna u sustavu videonadzora je određivanje minimalne potrebne memorije tvrdog diska za pohranu snimki video kamera. Takav izračun ovisi o brzini prijenosa podataka

(eng. bitrate), količini kamera te vremenu za koje je potrebno snimati i sačuvati snimke prije brisanja. Bitrate se u videonadzoru odnosi na količinu podataka koja se prenosi ili pohranjuje, obično izražena u kilobitima ili megabitima po sekundi (Kbps ili Mbps). Na iznos bitrate-a utječe veličina jedne komprimirane slike i brzine kadra, tj. broj slika u sekundi, dok veličina komprimirane slike ovisi o razlučivosti kamere, odabranoj vrsti i stupnju kompresije (kvaliteti slike) te dinamici promatrane scene. Iz tog razloga, točan iznos veličine komprimirane slike teško je dobiti pomoću računskih metoda te se uzimaju deklarirani podaci proizvođača. Izračun brzine prijenosa podataka dan je izrazom:

$$Bitrate = veličina\ komprimirane\ slike\ [KB] \cdot brzina\ kadra\ [fps], \qquad (4.2)$$

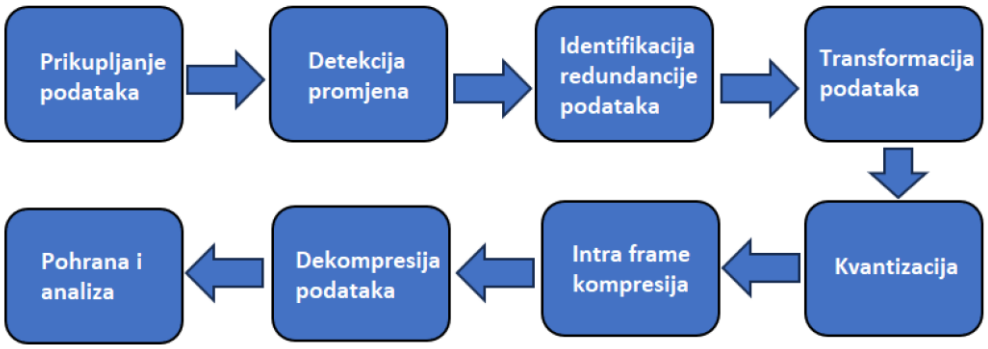
a za određivanje minimalne potrebne memorije tvrdog diska koristi se izraz:

$$Ukupna\ memorija = broj\ kamera \cdot bitrate[Mbps] \cdot vrijeme[s]. \qquad (4.3)$$

Ukupna memorija obično je izražena u gigabajtima ili terabajtima (GB ili TB). U svrhe odabira optimalnog tvrdog diska nužno je poznavati minimalnu vrijednost memorije potrebnu za pohranu snimki određenog sustava videonadzora.

4.2.1. Kompresija videozapisa

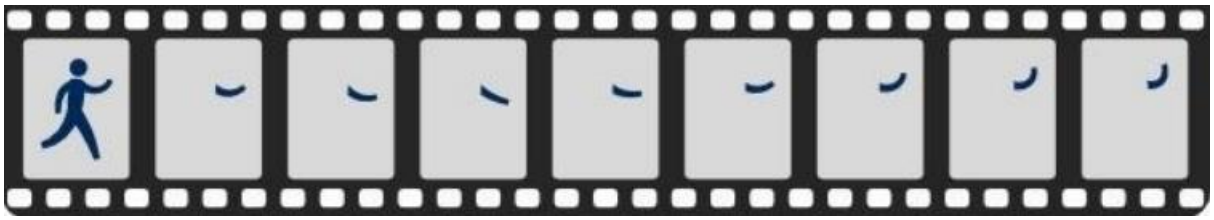
Kompresija videozapisa je tehnologija koja omogućuje učinkovitu pohranu, prijenos i obradu video sadržaja. IP kamere generiraju velike količine videozapisa, a kompresija videozapisa smanjuje veličinu tih videozapisa kako bi se olakšalo njihovo upravljanje i prijenos. Kompresija videa u sustavu videonadzora složen je proces (slika 4.29.) koji započinje s prikupljanjem podataka video sadržaja koji se sastoji od kadrova prikazanih u nizu jedan za drugim.



Slika 4.29. Proces kompresija videa

Nakon što se iz svakog kadra prikupe karakteristike kao što su boja i svjetlina, računalni algoritmi identificiraju redundanciju podataka, tj. ponavljanje informacija ili sličnost s prethodnim

dijelovima snimke u svrhe predviđanja. Primjer toga je videozapis s malo promjena u sceni gdje algoritam može pretpostaviti da će kadrovi koji slijede biti slični te odmah smanjiti količinu podataka za pohranu. Idući korak je transformacija podataka iz vremenske u frekvencijsku domenu pomoću diskretne kosinusne transformacije ili DCT (eng. Discrete Cosine Transform) radi prepoznavanja dijelova videa koji se ponavljaju i dijelova videa koji se mogu dodatno komprimirati. U procesu kvantizacije određuje se količina informacija koja se čuva, kao i onih koje se brišu. Korak od posebne važnosti u sustavima videonadzora je *Intra frame* ili *I-frame* kompresija, prikazan slikom 4.30.



Slika 4.30. Intra frame kompresija [40]

Ovaj korak bilježi sličnosti između niza kadrova i pohranjuje isključivo razlike među njima, tj. šalje se jedna potpuna slika (I-frame) koju slijedi niz djelomičnih slika (P-frame) što rezultira smanjenjem ukupne količine podataka. Podaci se pohranjuju na uređaj ili prenose putem mreže tek nakon kompresije, a proces dekompresije odvija se na uređaju za pregled snimke. [41]

Postoje različite metode kompresije koje se koriste u sustavima IP videonadzora, a to su MPEG-4, MJPEG, H-264 i H.265. MPEG-4 je stariji standard kompresije koji je i dalje prisutan u nekim IP kamerama i uređajima. Metoda koja komprimirani video sadržaj prikazuje kao niz pojedinačnih slika poznatih kao JPEG slike zove se MJPEG kompresija. Ova metoda može pružiti dobru kvalitetu slike, ali obično generira veće datoteke u usporedbi s H.264 i H.265. H.264 ili AVC jedan je od najčešće korištenih standarda kompresije videa koji koristi različite tehnike za smanjenje redundancije podataka i optimizaciju kompresije. Nasljednik H.264 tehnologije koji nudi još bolji omjer kompresije, pružajući visoku kvalitetu slike uz manje potrebnog prostora za pohranu zove se H.265 ili HEVC (eng. High Efficiency Video Coding). Ova metoda kompresije posebno je bitna pri prijenosu visokokvalitetnih videozapisa putem interneta ili mreže s ograničenom propusnosti (eng. bandwidth), a usporedba s H.264 dana je tablicom 4.3.

Tablica 4.3. Usporedba H.264 i H.265 kompresija [42]

Vrsta kompresije	Razlučivost	Potreban bandwidth [Mbps]
H.264 (AVC)	640x480 (480p)	1,5
	1080x720 (720p)	3
	1920x1080 (1080p)	6
	4096x2160 (4k)	32
H.265 (HEVC)	640x480 (480p)	0,75
	1080x720 (720p)	1,5
	1920x1080 (1080p)	3
	4096x2160 (4k)	15

Kao što je vidljivo iz tablice, H.265 kompresija za istu razlučivost ima dvostruko manju propusnost od H.264 što rezultira datotekama upola manje veličine uz približno jednaku kvalitetu slike. Jedina mana je što veća učinkovitost H.265 zahtijeva veću računalnu snagu što s vremenom prestaje biti problem.

Jedna od karakteristika video snimača je dodjeljivanje različitih varijacija video sadržaja (eng. stream) koje se mogu prilagoditi prema potrebama korisnika. IP kamere često pružaju mogućnost istovremenog slanja više video streamova različitih razlučivost, brzina kadrova te stupnja i vrste kompresije. Uobičajeni tipovi streamova u video snimačima su glavni stream i dvije razine podređenog streama. Glavni (eng. Main) stream pruža najveću razlučivost, najviši frame rate i najbolju kvalitetu slike te se uobičajeno koristi za pohranu snimki. Česte postavke u main streamu video snimača su Full HD razlučivost, 20 fps brzina kadrova i H.265 kompresija videa. S druge strane, podređeni ili sub stream obično ima smanjenu kompresiju videa u odnosu na glavni stream te se u koristi u situacijama s manje dostupnom propusnosti mreže za pregled scene uživo (eng. Live View). Postavke ovog streama u praksi su uglavnom HD razlučivost, 25 fps i H.264 kompresiju, gdje veliki fps rezultira preglednijom scenom, posebice u dinamičnim scenama. Drugu razinu podređenog streama karakterizira najmanja kvaliteta slike i brzina kadrova te takav stream obično ima VGA razlučivost, 15 fps i H.264 kompresiju. Svaki od streamova podložan je izmjenama u postavkama, bilo promjenom razlučivosti, brzine kadrova ili kompresije, kako bi se zadovoljili zahtjevi korisnika.

Mrežni video snimači standardno se koriste za manje sustave IP videonadzora, dok se za sustave s većim brojem IP kamera koji zahtijevaju specijalne funkcije koriste IT (eng. Information

technology) serveri. Za razliku od mrežnih snimača, IT serveri imaju dodatne komponente kao što je grafička kartica te su po konstrukciji zahtjevniji i skuplji. Serveri su računala s Windows operativnim sustavom čija je zadaća spremanje video sadržaja i izvođenje aplikacije za rad s kamerama. Kao i kod snimača, na server se također povezuje preko web preglednika ili zasebne klijentske aplikacije. Smjer razvoja IP kamera je takav da centralni uređaj više nije nužno potreban. Sama kamera je inteligentna, sama određuje alarmno stanje koristeći inteligentnu analizu slike ili alarmne ulaze. U slučaju alarmnog stanja, snimka se zapisuje na memorijsku karticu koja se nalazi unutar sklopa kamere čime prijenos slike nije potreban. Može se reći da se inteligencija i procesiranje podataka sele iz centraliziranog u periferni sustav što je važna značajka mrežnog sustava videonadzora. Sa sigurnosnog aspekta, snimanje samo na kameri nije poželjno budući da se tako videozapis izlaže mogućem uništenju ili otuđivanju uslijed vanjskih čimbenika. Iz tog razloga, osim lokalnog snimanja IP kamere se povezuju ili na lokalnu pohranu ili danas sve popularniji cloud način pohrane, gdje se snimač nalazi u podatkovnom centru (eng. data center) i kamera mu šalje video signal putem Interneta. Osim opcija snimanja kamera se može programirati i da samostalno šalje elektroničku poštu u slučaju incidentne situacije ili šalje poruku putem SNMP (eng. Simple Network Management Protocol) protokola. Dakle, mrežne kamere su "mala računala“ koja komuniciraju koristeći računalnu mrežu. Kad je korištenje resursa mreže u pitanju jedna ih činjenica značajno razlikuje od osobnih računala, a to je faktor istovremenosti. Osobno računalo mrežni priključak koristi povremeno dok većinu vremena ne generira promet na mreži. Iznimka su trenuci gledanja filmova ili preuzimanja velike količine podataka pri kojima kroz mrežu neprekidno putuju podaci. Isti je slučaj s mrežnom kamerom koja neprekidno generira mrežni promet uslijed aktivne promatrane scene i tako troši mrežne resurse. Iznimka su kamere koje imaju detekciju alarmnog stanja na samoj kameri te generiraju mrežni promet samo onda kada je u pitanju alarmno stanje i tada šalju video podatke na mjesto snimanja. U slučaju da se detekcija odvija na snimaču, svaka kamera neprekidno će generirati promet u računalnoj mreži. Kada se radi o većem broju kamera tu činjenicu itekako treba uzeti u obzir. Tu se opet naglašava važnost poznavanja projektiranja i izvođenja računalnih mreža kako bi mreža mogla omogućiti nesmetan rad sustava za videonadzor. Iz tog se razloga preporučuje izgradnja potpuno odvojene računalne mreže za videonadzor i tehničku zaštitu, mreže koja je i fizički i adresno odvojena od matične računalne mreže objekta koji se štiti. [43]

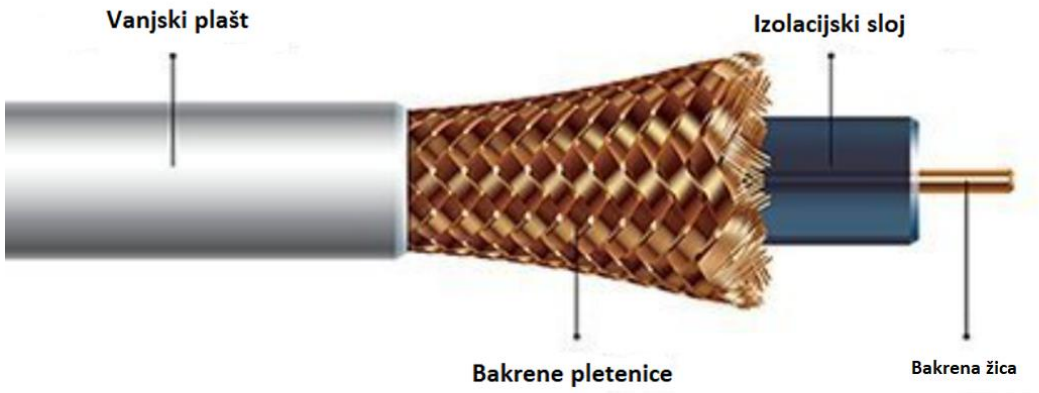
4.3. Prijenos signala i mrežna infrastruktura

U sustavima videonadzora, prijenos signala od kamera do snimača ili centralnog sustava može se ostvariti na nekoliko načina. Jedan od tradicionalnih načina je analogni žičani prijenos, u kojem kamere šalju analogni video signal putem koaksijalnih kabela do snimača. Suvremeni sustavi sve

više koriste digitalne IP kamere koje prenose video signal putem mrežnih Ethernet kabela, upletenih parica ili optičkog kabela. Također, u situacijama gdje žično povezivanje nije praktično postoji mogućnost bežičnog prijenosa video signala putem standardne bežične mrežne komunikacije.

4.3.1. Analogno povezivanje

Tradicionalni sustavi videonadzora koriste analogni prijenos signala putem koaksijalnog kabela. Koaksijalni kabel sastoji se od tanke bakrene žice omotane izolacijskim slojem neke vrste dielektrika, vanjskog oklopa sastavljenog od bakrenih pletenica ili aluminijske folije te vanjskog plašta, kao što je prikazano na slici 4.31. [44]



Slika 4.31. Sastav koaksijalnog kabela [45]

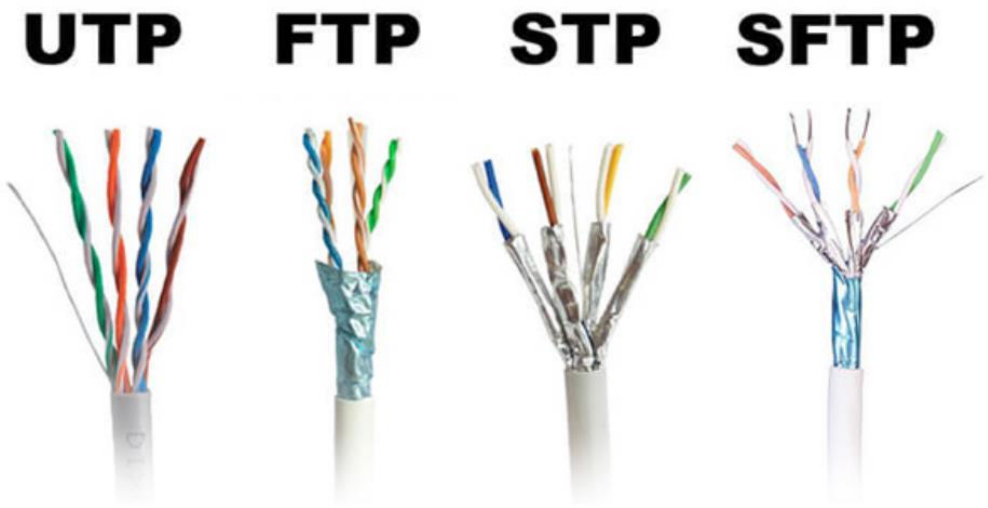
Izolacijski sloj služi za sprječavanje gubitka signala dok vanjski plašt služi kao zaštita od oštećenja, vremenskih uvjeta te nametnika. Ovakva struktura omogućuje otpornost koaksijalnog kabela na elektromagnetske smetnje i vanjske utjecaje. Dvije vrste koaksijalnog kabela koje se najviše koriste u videonadzoru su RG11 i RG59. Maksimalna dopuštena duljina RG59 kabela je 500 m, odnosno 300 m za RG11 kabel. Na slici 4.32. prikazan je BNC konektor koaksijalnog kabela.

Slika 4.32. Izgled BNC konektora[46]

Koaksijalni kabel se za prijenos signala i dalje koristi u sustavima videonadzora, posebno u postojećim instalacijama koje su izgrađene prije pojave IP kamera te za AHD (eng. analog HD) tehnologiju visoke razlučivosti. Međutim, zbog mnogobrojnih prednosti nad analognim videonadzorom, sve više korisnika prelazi na mrežne sustave videonadzora što je dovelo do znatnog smanjenja njegove upotrebe u novijim instalacijama.

4.3.2. IP mrežno povezivanje

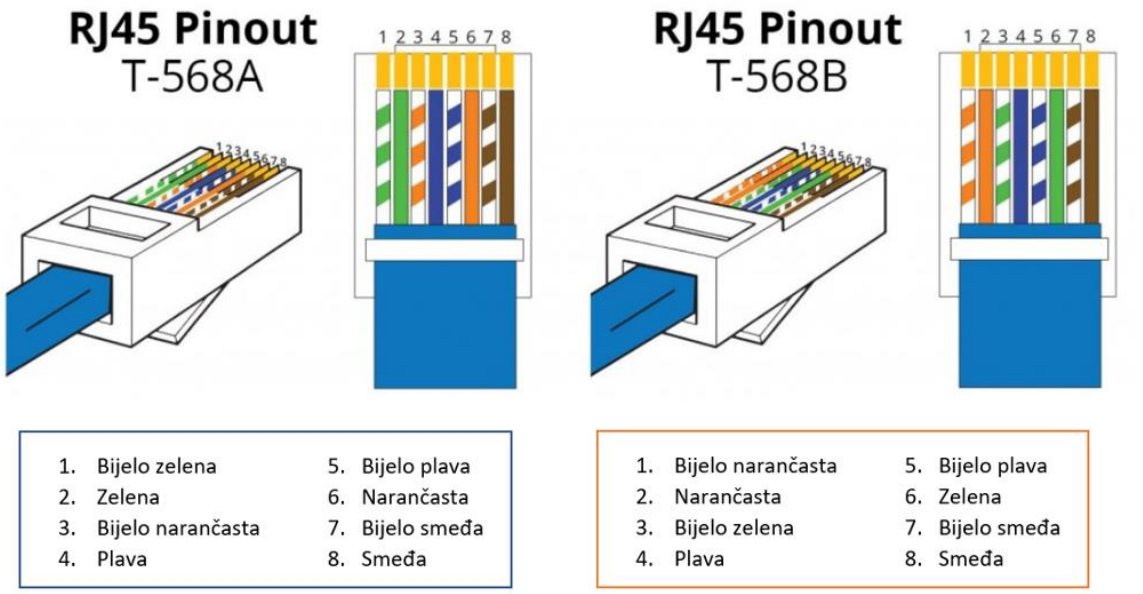
IP kamere koriste Ethernet kabele ili bežičnu mrežu za prijenos video signala do mrežnog snimača ili video upravljačkog sustava. Mediji za prijenos video signala žičanim putem su upletene parice ili optički kabel. Upletene parice najzastupljeniji su način kabliranja u svrhe povezivanja uređaja unutar sustava videonadzora. Vidljivo sa slike 4.33., postoje četiri vrste upletenih parica: UTP, FTP, STP i SFTP.



Slika 4.33. Vrste upletenih parica [47]

Neoklopljena upletena parica ili UTP (eng. Unshielded Twisted Pair) sastoji se od četiri para upletenih i izoliranih bakrenih žica te vanjskog omotača. Razlog upletenosti žica je smanjenje stvaranja smetnji među žicama uzrokovanih visokim frekvencijama (engl. Crosstalk) ili vanjske interferencije. U slučaju kada je potrebna veća zaštita bakrenih žica od elektromagnetskih smetnji i vanjskih utjecaja, koristi se FTP (eng. Foiled Twister Pair), STP (eng. Shielded Twisted Pair) ili SFTP (eng. Shielded Foiled Twisted Pair) kabel. Također, postoji tip kabela za vanjske instalacije s dodatnom zaštitom od glodavaca, UV zračenja, i vremenskih uvjeta pod nazivom Outdoor UTP kabel. Takav kabel pogodan je za postavljanje pod zemljom te se koristi za međusobno povezivanje uređaja u udaljenim objektima. [48]

U mrežnoj infrastrukturi sve četiri vrste kabela upletenih parica koriste RJ-45 konektor, čija je funkcija uspostavljanje fizičke veze između uređaja, poput računala ili mrežnih uređaja, i Ethernet mreže. Za spajanje uređaja pomoću upletenih parica postoje dva različita standarda povezivanja, T-568A i T-568B, a njihov način spajanja prikazan je slikom 4.34. [49]



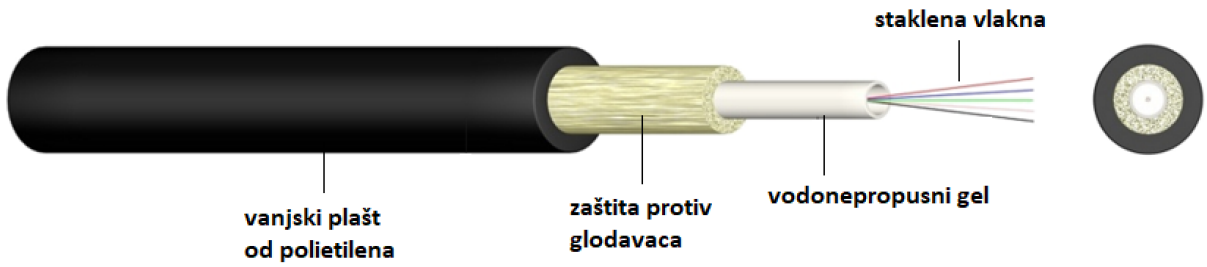
Slika 4.34. Standardi za spajanje uređaja [50]

Iako mnogi uređaji podržavaju T-568A način spajanja, u sustavima videonadzora gotovo uvijek se koristi T-568B standard. Postoji nekoliko standarda vezanih za UTP kabele, a najpoznatiji su definirani kategorijama (CAT). Ti standardi određuju karakteristike kabela u smislu propusnosti, performansi i sposobnosti neometanog slanja signala, koje su prikazane tablicom 4.4.

Tablica 4.4. Kategorije kabela [51]

Kategorija kabela	Brzina prijenosa podataka [Mbps]	Frekvencija signala [MHz]	Primjena
CAT5	10^2	100	Telefonske linije, nezahtjevne kućne i poslovne mreže
CAT5E	10^2	100	VoIP (eng. Voice over IP), kućne mreže, manje zahtjevna poslovna okruženja
CAT6	10^3	250	Poslovne mreže, kućne mreže većih zahtjeva, prijenos video signala
CAT6A	10^4	500	Poslovne mreže, podatkovni centri, zahtjevne aplikacije
CAT7	10^4	600	Podatkovni centri, zahtjevne poslovne mreže, profesionalne video i audio aplikacije

CAT5E (unaprijeđeni CAT5) ima bolje performanse i zaštitu od ometanja signala od CAT5 kabela, dok CAT6 ima bolju propusnost, smanjene smetnje i bolju zaštitu od CAT5E. Naprednije kategorije, poput CAT6 i CAT7, ostvaruju maksimalnu duljinu prijenosa signala od 100 metara pri korištenju brzine prijenosa do 1Gbps, gdje CAT7 karakterizira visoka propusnost i dodatna zaštita od ometanja. Međutim, kada su u pitanju brzine prijenosa od 10, 25 ili 40 Gbps, maksimalna udaljenost se obično skraćuje kako bi se očuvala kvaliteta signala. Kao što se može primijetiti, duljina kabela izravno utječe na kvalitetu signala, gdje s duljim kabelom dolazi do gubitka signala i smanjene brzine prijenosa. Iz tog razloga, ako je potrebno omogućiti povezivanje uređaja na većim udaljenostima od 100 metara, poželjno je razmotriti uporabu drugih tehnologija poput optičkih vlakana. [51] Zbog mnogih prednosti nad bakrenom žicom sve više se u modernim sustavima videonadzora koristi optički kabel. Ovaj medij za prijenos informacija umjesto električnih signala koristi svjetlosne signale što ga čini otpornim na elektromagnetsku interferenciju. Kao što je vidljivo sa slike 4.35., optički kabel sastoji se od optičkih vlakana okruženih staklenim ili plastičnim omotačem čija je uloga zadržavanje svjetlosti unutar kabela.



Slika 4.35. Sastav optičkog kabela [52]

Također, radi zaštite od glodavaca i vlage optički kabel najčešće sadrži sloj čelične armature i vodonepropusnog gela. Kako bi se omogućilo povezivanje vlakana optičkog kabela s drugim optičkim komponentama i uređajima koriste se posebne vrste konektora. Najčešće korišteni konektori u sustavima videonadzora su SC (eng. Subscriber Connector) i LC (eng. Lucent Connector), gdje je zbog jednostavnosti i pouzdanosti najrasprostranjeniji SC konektor. Oba konektora imaju push-pull mehanizam koji omogućuje brzo umetanje i izvlačenje konektora bez dodatnih alata. Kao što je prikazano slikom 4.36., SC konektor kvadratnog je oblika te koristi keramičku ili metalnu pločicu za centriranje optičkog vlakna. [53]

Slika 4.36. Prikaz SC konektora[54]

Na slici 4.37. prikazan je LC konektor. Izgledom je vrlo je sličan SC konektoru, samo manji po veličini čime ostvaruje veću gustoću povezivanja mrežne opreme.

Slika 4.37. Prikaz LC konektora [55]

Zbog velike propusnosti, optički kabeli omogućuju prijenos velike količine podataka u kratkom vremenskom razdoblju. Svjetlosni signali manje su osjetljivi na smetnje i gubitke signala tijekom prijenosa na velikim udaljenostima u usporedbi s električnim signalima u bakrenoj žici. Budući da su optički kabeli otporni na elektromagnetske smetnje, pružaju sigurniji i pouzdaniji prijenos podataka. Također, otporni su na mehanička djelovanja te se mogu koristiti u opasnim okruženjima gdje ne smije doći do iskrenja. Isto tako, tanji su i lakši od bakrenih kabela, što olakšava njihovu instalaciju i rukovanje. Danas je optički kabel sve financijski pristupačniji te su sve više u upotrebi i za manje udaljenosti.

4.3.3. Usporedba medija za prijenos signala

Ovisno o brzini prijenosa podataka, optički kabel podržava brzine do nekoliko terabita u sekundi što je znatno više od koaksijalnog kabela ili upletenih parica, gdje upletene parice često karakterizira najsporiju brzinu prijenosa. S obzirom na udaljenost na kojoj se signal prenosi, optički kabel je također najbolja varijanta s mogućnosti prijenosa do više desetaka kilometara. Osim u slučaju korištenja PoE (eng. Power over Ethernet) tehnologije, upletene parice ograničene su na udaljenosti oko stotinu metara, čime su lošiji medij i od koaksijalnog kabela. PoE tehnologija omogućuje prijenos električne energije i komunikacije putom iste fleksibilne upletene parice što u usporedbi s krućim koaksijalnim kabelom znatno olakšava i ubrzava instalaciju. Još jedna u nizu prednosti optičkog kabela u odnosu na upletene parice i koaksijalni kabel je i potpuna otpornost na elektromagnetske smetnje ostvarena korištenjem svjetlosnog signala za prijenos podataka. Jedina stavka zbog koje optički kabel nije i dalje u potpunosti zamijenio ostale su njegova visoka cijena te otežana instalacija i održavanje. Upletene parice najjeftinija su opcija kabliranja uz jednostavnu instalaciju i integraciju s mrežom, što olakšava upravljanje i nadzor sustava.

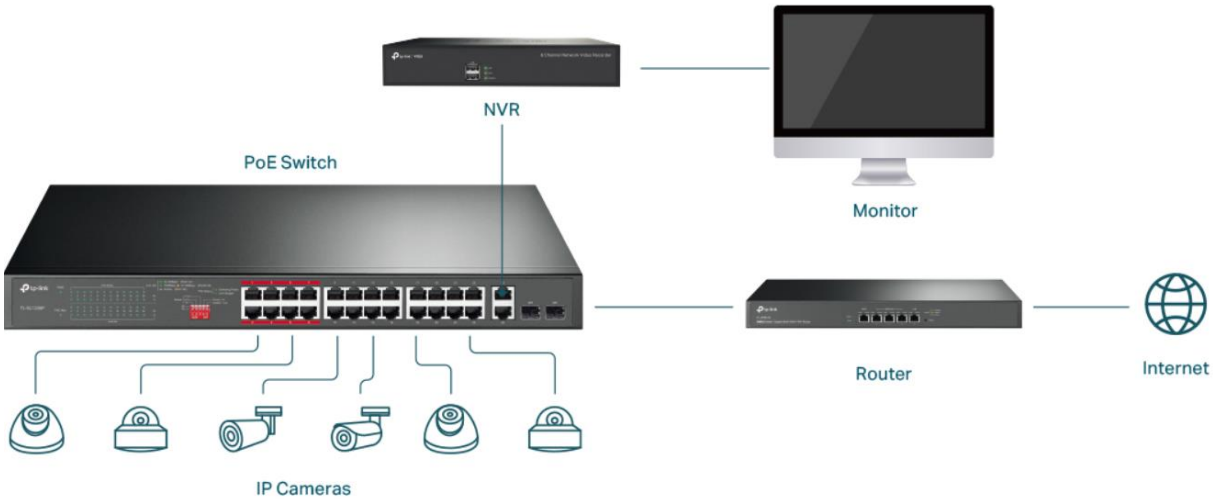
4.3.4. Bežični prijenos signala

Bežični LAN ili WLAN (eng. Wireless LAN) sustavi omogućuju komunikaciju mrežnih uređaja i pristup na mrežu služeći se radiosignalima kao transportnim medijem. Bežična mreža može biti priključena na postojeći žičani LAN kao proširenje ili može činiti osnovu za potpuno novu mrežu. Zbog nekorištenja kabela, bežični sustav fleksibilniji je i jednostavniji te zahtjeva znatno manje vrijeme instalacije od žičanog. Iako primjenjivi i za vanjske instalacije, WLAN-ovi su posebno pogodni za unutarnje instalacije pogotovo na mjestima gdje je žičana infrastruktura teško izvediva. S druge strane, kako bi sustav radio stabilno potrebna je pouzdana bežična mreža čija je izgradnja često skupa. Također, za razliku od žičanog, bežičnim sustavom ograničava se brzina prijenosa podataka što u slučaju velike količine podataka može rezultirati smanjenom kvalitetom snimane scene. Isto tako, ovi sustavi osjetljiviji su na vanjske prijetnje kao što je hakiranje čime dolazi do narušavanja privatnosti i gubitka povjerljivih podataka. Iz navedenih razloga, bežična infrastruktura zastupljena je ponajviše u malim poslovnim objektima, privatnim kućama i stanovima te mobilnim objektima, dok se na većim objektima poput poslovnih zgrada, financijskih institucija i javnih objekta gotovo uvijek upotrebljava žičana infrastruktura. [56]

4.4. Mrežni preklopnik

Mrežni preklopnik (eng. network switches) igraju ključnu ulogu u sustavima videonadzora. Kao što je vidljivo sa slike 4.38. mrežni preklopnici omogućuju povezivanje i komunikaciju između

različitih mrežnih uređaja, uključujući IP kamere, video snimače, video servere i druge uređaje u mreži. U slučaju da se želi omogućiti pristup sustavu i IP uređajima preko interneta, potrebno je u postojeći sustav dodati ruter čija je glavna funkcija usmjeravanje podataka između različitih mreža.



Slika 4.38. Mrežni preklopnik u sustavu videonadzora [57]

Glavni dijelovi mrežnog preklopnika su mrežni ulazi (eng. ports), CPU, memorija, napajanje i LED indikatori. Portovi služe za povezivanje preklopnika s različitim mrežnim uređajima pomoću kabela. Posebna vrsta porta je konzolni port koji omogućuje administratorski pristup za konfiguraciju i dijagnostiku samog switch-a. Pomoću CPU-a obrađuju se podaci i upravlja preusmjeravanjem podatkovnog prometa na odgovarajuće portove, a za privremeno pohranjivanje informacija koristi se RAM. Također, mrežni preklopnik ima i internet sučelje koje omogućava administratorima upravljanje postavkama te ASIC (eng. Application-Specific Integrated Circuit) – posebno dizajnirani integrirani krug koji brzo i učinkovito preusmjerava podatke na preklopniku. [58]

4.4.1. Karakteristike mrežnog preklopnika

Prilikom odabira mrežnog preklopnika u sustavu videonadzora, važno je uzeti u obzir potrebe mreže, broj uređaja koji se spajaju na preklopnik, brzinu prijenosa podataka, sigurnosne zahtjeve i budžet. Brzina prijenosa podataka ili propusnost označava koliko podataka preklopnik može prenijeti u jedinici vremena. Mrežni preklopnici podržavaju različite brzine prijenosa, kao što su 1 Gbps, 10 Gbps, 100 Gbps i više, omogućujući prilagodbu potrebama mreže. Ovisno o broju

uređaja koje je potrebno povezati preko mrežnog preklopnika, nužno je imati mrežni preklopnik s pripadajućim brojem portova. S obzirom na vrstu upravljanja razlikuju se dvije vrste preklopnika, upravljani preklopnici koji omogućuje napredno upravljanje mrežom putem različitih postavka i neupravljani koji se obično koriste u manjim mrežama i jednostavniji su za rukovanje od upravljanih. PoE preklopnici osiguravaju napajanje IP uređaja u sustavu putem istog Ethernet kabela korištenog za komunikaciju uređaja što smanjuje potrebu za dodatnim kabliranjem. Visoka propusnost i pouzdanost mrežnih preklopnika od velike su važnosti kako bi se osigurao brzi i stabilni prijenos video signala. [59]

5. VIDEOANALITIKA

Videoanalitika u sustavu videonadzora je tehnologija koja koristi napredne algoritme i programske alate kako bi automatski analizirala video snimke. Ova tehnologija omogućuje detekciju, prepoznavanje, praćenje i izvlačenje korisnih informacija iz velike količine video materijala. Umjesto da ljudi moraju ručno pregledavati i analizirati sate i sate videozapisa, videoanalitika to može učiniti mnogo brže i preciznije. Postoje raznolike funkcije i primjene videoanalitike kao što su detekcija pokreta (ljudi i vozila), detekcija i prepoznavanje lica, brojanje ljudi i vozila, prepoznavanje registarskih oznaka vozila, praćenje prelaska preko linija i ulazak u zone, analiza prometa i ponašanja itd. Sve navedene vrste videoanalitike podrazumijevaju visoki stupanj točnosti i pouzdanosti kako bi njihova implementacija u video kamerama ili snimačima ostvarila zahtjeve korisnika. [60]

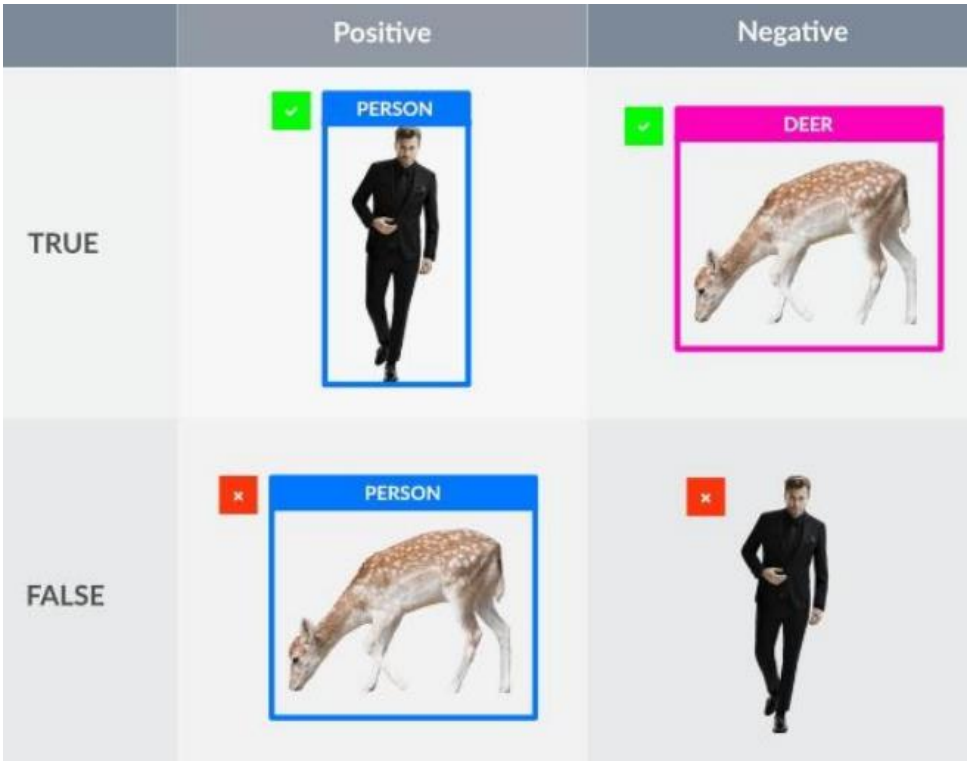
5.1. Točnost videoanalitike

Točnost mjerenja u videoanalitici odnosi se na mjeru koliko kvalitetno algoritam ili sustav za analizu videa identificira, kategorizira i prati objekte, događaje ili karakteristike u stvarnom svijetu. Točnost se na osnovi referentnog skupa podataka može mjeriti koristeći različite metrike i kriterije, a jednostavnije će biti obrađene u nastavku. U videoanalitici, referentni skup podataka koji se koristi za evaluaciju i validaciju različitih algoritama i tehnika analize podataka zove se temeljna istina (eng. ground truth). Umjesto pretpostavki i zaključivanja, temeljna istina se koristi za opisivanje informacija prikupljenih putem direktnog promatranja. Uobičajeni primjer je broj kuglica unutar staklene posude. Algoritam može procijeniti koliko kuglica se nalazi u posudi pomoću procjene veličine jedne kuglice i volumena posude, dok temeljna istina zahtijeva prebrojavanje svake kuglice od strane osobe izvlačenjem iz posude. U videonadzoru, temeljna istina se postiže vizualnom potvrdom rezultata analitike snimanog sadržaja što je jedini način utvrđivanja vjerodostojnosti analitike, tj. da li analitika detektira ono što treba, propušta objekte ili griješi. Određivanje „ground truth“ vrijednosti za alarmna stanja je jednostavno jer sustav u tom trenutku automatski generira videozapis za pregled i klasifikaciju ispravnosti. Međutim, određivanje „ground truth“ vrijednosti u situacijama gdje objekti nisu detektirani je znatno zahtjevnije. Razlog tome je što sustav tada ne stvara upozorenje te je potrebno pregledati sve videozapise što praktično uništava svrhu korištenja analitike. Još jedan primjer otežanog određivanja temeljne istine su kamere za detekciju povišene tjelesne temperature što bi za provjeru zahtijevalo ručno mjerenje temperatura svih osoba. [61]

Sve analitike se sastoji od četiri osnovna ishoda koji utječu na točnost performansi sustava, a to su:

- stvarno pozitivni (eng. True Positives),
- stvarno negativni (eng. True Negatives),
- lažno pozitivni (eng. False Positives) i
- lažno negativni rezultati (eng. False Negatives).

Za primjer će se uzeti analitika za detekciju osoba, prikazano slikom 5.1.



Slika 5.1. Osnovni ishodi točnosti [62]

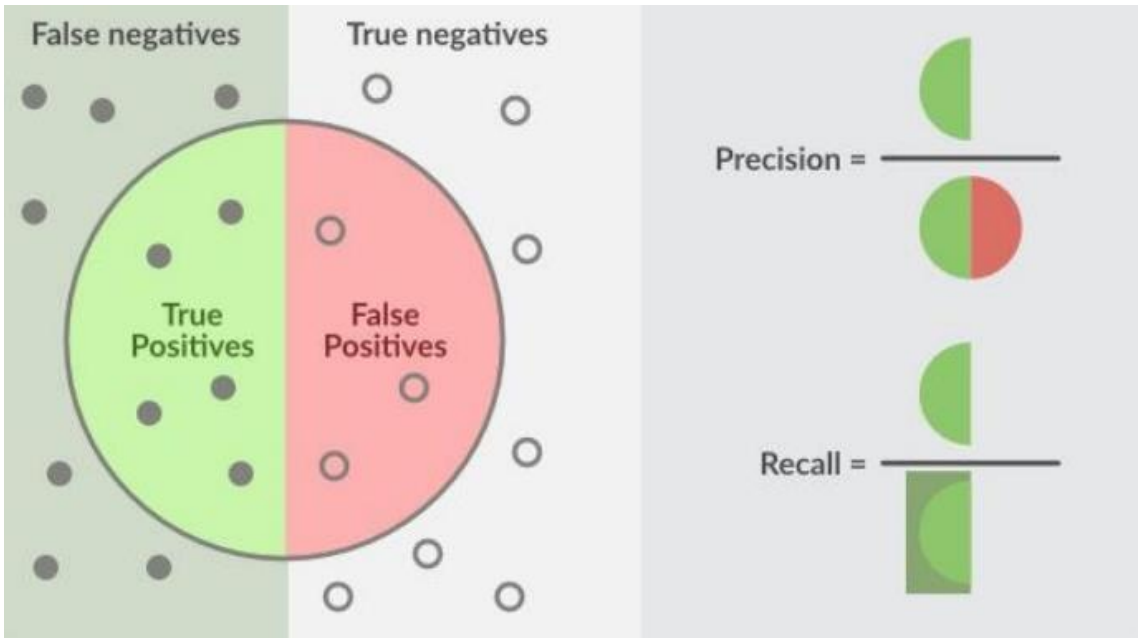
U slučaju stvarno pozitivnih rezultata, osoba će biti detektirana kao osoba, dok za stvarno negativne rezultate, životinja neće biti detektirana kao osoba. Lažno pozitivni rezultat identificirat će životinju kao čovjeka, a lažno negativni uopće neće detektirati osobu. S obzirom na ove rezultate, moguće je izračunati točnost analitike dane izrazom:

$$Točnost = \frac{broj\ svih\ događaja\ -\ broj\ negativnih\ događaja}{broj\ svih\ događaja}. \qquad (5.1)$$

Međutim, ovakav pojednostavljeni izračun točnosti ima ograničenu vrijednost u analizi ukupnih performanse algoritma. Na primjer, ako je algoritam za detekciju oružja obradio 100 osoba i pritom nije otkrio niti jedno oružje, ali 5 osoba je imalo oružje, prema ovom izračunu se dobiva točnost od 95%, bez obzira na to što se oružje nije uopće detektiralo. Iz tog razloga, pri treniranju algoritma potrebno je u obzir uzeti mnoge različite faktore koje utječu na procjenu točnosti.

5.1.1. Preciznost i odziv

Zbog ograničenja pri korištenju pojednostavljenih izračuna točnosti, postoje dva osnovna načina određivanja kvalitete algoritma, a to su preciznost (eng. Precision) i odziv (eng. Recall). Preciznost mjeri koliko je često prepoznati objekt točan (npr. osoba je stvarno osoba), tj. računa omjer stvarno pozitivnih i ukupno pozitivnih kao što je vidljivo sa slike 5.2.



Slika 5.2. Preciznost i odziv [63]

Odziv je mjera koliko točno analitika detektira sve objekte (npr. sve osobe, sva lica, sva vozila), a određuje se kao omjer stvarno pozitivnih i zbroja stvarno pozitivnih i lažno negativnih rezultata. S porastom lažno pozitivnih rezultata preciznost se smanjuje, dok se odziv smanjuje pri porastu lažno negativnih rezultata. Preciznost predstavlja koliko dobro algoritam ispravno pronalazi objekte, ali ne uzima u obzir objekte koje propušta (lažno negativne) ili ispravno ignorira (stvarno negativne). Sustavi za kontrolu pristupa prepoznavanjem lica zahtijevaju visoku preciznost kako ne bi omogućili pristup pogrešnoj osobi, gdje lažno negativni rezultati značajno utječu na takav sustav. Za primjer će se uzeti testiranje algoritma za detekciju oružja na skupu podataka od 10000 ljudi. Iako je algoritam detektirao oružje kod četvero ljudi, samo jedna osoba je posjedovala oružje, a 25 ljudi s oružjem uopće nije detektirano. Preciznost takvog algoritma dobivena je izrazom:

$$Preciznost = \frac{stvarno\ pozitivni}{ukupno\ pozitivni} = \frac{stvarni\ broj\ oružja\ iz\ detektiranog\ skupa}{broj\ detektiranih\ oružja}$$

$$= \frac{1}{4} = 0{,}25. \qquad (5.2)$$

Odziv predstavlja koliko dobro algoritam detektira sve promatrane objekte, ali ne uzima u obzir koliko dobro ispravno ignorira objekte ili koliko ih netočno identificira. Odziv se vrlo često koristi za procjenu točnosti algoritma, posebno kada je potrebno ispravno detektirati stvarne pozitivne rezultate. [64] Na primjeru iznad, pri detekciji oružja odziv se dobiva izrazom:

$$Odziv = \frac{stvarno\ pozitivni}{stvarno\ pozitivni + lažno\ negativnih} = \frac{1}{1+25} \sim 0{,}04. \qquad (5.3)$$

5.2. Detekcija objekta

Detekcija objekta u videoanalitici tehnika je obrade video sadržaja pomoću računalnih algoritama i tehnologija poput strojnog učenja za identifikaciju i praćenje. Ova tehnika omogućava računalima da automatski prepoznaju prisutnost određenih objekta, poput ljudi, vozila, životinja, predmeta ili drugih entiteta, te da prate i analiziraju njihovo ponašanje.

5.2.1. Detekcija ljudi, lica i vozila

U videoanalitici, detekcija ljudi, lica ili vozila tehnika je obrade videozapisa koja se koristi za automatsko prepoznavanje i lokalizaciju podataka koji se obično prikupljaju uživo sa sigurnosnih kamera ili iz arhive snimljenih materijala. Takav videozapis cjepka se na kadrove ili slike čime se omogućava analiza svakog kadra zasebno. Analiza se vrši pomoću raznih algoritama, a najuspješniji su algoritmi temeljeni na strojnom i dubokom učenju. Detekcija temeljena na strojnom učenju najčešća je na IP kamerama zbog brzine procesiranja koja u odnosu na duboko učenje zahtijeva manje vrijeme što je ključno za upozorenja u realnom vremenu. U trenutku detekcije, algoritam vraća koordinate pravokutnika (eng. bounding box) oko određenog lica, čovjeka ili vozila u svakom kadru čime se izvršava lokalizacija podataka. Nakon detekcije i lokalizacije podataka, na njih se mogu primijeniti razne vrste analitike kao što je prepoznavanje lica, brojanje i praćenje osoba ili vozila, prepoznavanje ljudskih emocija, itd. Dobiveni rezultati mogu služiti kao alarmno stanje u stvarnom vremenu, ako se radi o kriminalcu ili nestaloj osobi, ili se mogu koristiti za dugoročnu analizu. Ova tehnika ima široku primjenu u različitim područjima sigurnosti, nadzora i identifikacije, gdje korištenje određenog algoritma uvjetuje karakteristikama promatrane scene. Osim što su algoritmi temeljeni na strojnom učenju brži od dubokog učenja, često su manje točni, posebno u uvjetima ograničenog vidokruga i promjenjivih osvjetljenja koji su uobičajeni u sustavima videonadzora. Nužno je razlikovati detekciju, koja pronalazi lice, od prepoznavanja, koje određuje kome to lice pripada. Iako je detekcija izazovna, znatno je jednostavnija metoda od prepoznavanja lica. Neuspješna detekcija lica obično znači da se lice nije prepoznalo kao dio ljudske glave, dok neuspješno prepoznavanje lica može rezultirati pogrešno identificiranom osobom prilikom istraživanja zločina. Premda su to dvije različite

analitike, prepoznavanje lica direktno ovisi o efikasnosti detekcije te se izvršava isključivo nakon uspješne detekcije lica. Detekcija ljudskog lica zahtijeva 10 puta uže vidno polje, tj. 10 puta veću gustoću piksela ili PPM (eng. pixels per meter) u odnosu na detekciju osoba, dok se vozila mogu detektirati u dvostruko širem vidnom polju u odnosu na osobe. Na primjeru prikazanom slikom 5.3., sa streamom podataka Full HD razlučivosti, lica se mogu detektirati do širine scene od 7 metara, osobe se mogu detektirati do širine od 70 metara, a vozila do 140 metara. [65]

Slika 5.3. Detekcija objekta ovisno o širini scene [66]

Problematika vezana za detekciju osoba leži u okolišnim i logističkim izazovima. Iako su mnoge analitike za detekciju osoba precizne pri dobrom osvjetljenju i uz jasne detalje subjekta, postoje faktori koji uzrokuju greške. Zbog nepredvidive osvijetljenosti i vremenskih uvjeta, neki od tih faktora posebno su povezani s vanjskim videonadzorom. Nepovoljni vremenski uvjeti jedan su najčešćih izazova za analitiku, pri kojima je moguće prepoznavanje snijega i kiše kao osobe, vidljivo sa slike 5.4.

Slika 5.4. Primjer krive detekcije osobe [67]

Također, uzrok lažnih detekcija osoba su brze promjene u osvjetljenju ili pokretna svjetla, kao što su prednja svjetla na vozilu u pokretu. Zbog ograničenja analitika u mnogim kamera, neki sustavi za detekciju mogu propustiti osobu koja trči zato što se videozapis analizira pri niskoj vrijednosti fps-a (između 1-5 fps-a) gdje kamera ne prepoznaje objekt u pokretu kao osobu. Isto tako, mnoge analitike su naučene detektirati osobu u uspravnom položaju i to isključivo pri potpunoj vidljivosti osobe, što će rezultirati propustom u slučaju da osoba puže po podu ili je samo djelomično u kadru, kao što je prikazano na slici 5.5.

Slika 5.5. Nepostojanje detekcije pri djelomičnom prikazu osobe [68]

Iako je detekcija lica relativno česta u praksi, zbog malih dimenzija ljudske glave određivanje je li objekt u sceni lice znatno je izazovnije od pronalaska osobe ili vozila. Performanse koje uvelike utječu na kvalitetu detekcije lica su kut i osvjetljenje lica. Takva videoanalitika uglavnom lako detektira lice koje direktno gleda u kameru, dok s naginjanjem glave njena efikasnost značajno varira. Također, isti princip se odnosi i na osvjetljenje u promatranoj sceni, gdje se pri dobrom osvjetljenju lice lako prepoznaje, a otežano u uvjetima sjene, tame i šuma. Još jedan od problema je mjesto postavljanja videonadzora, pri kojem se većina kamera u praksi postavlja na stropove, uz zidove ili u kuteve prostorija. To rezultira djelomičnim slikama lica pri kojima je uglavnom vidljiva gornja strana glave ili češće kombinacija bočnog i gornjeg dijela glave. Detekcija ulaska i izlaska vozila iz promatranog područja ne suočava se s velikim brojem izazova te je znatno lakša metoda detekcije od prethodno navedenih. Najčešći izazov za detekciju vozila su često satima parkirana vozila, pri kojima mnoge analitike generiraju višestruka upozorenja za isto vozilo što brzo postaje smetnja pri nadzoru. Mnoge analitike bazirane na umjetnoj inteligenciji imaju sposobnost identifikacije vozila po tipu, bilo da se radi o automobilu, kamionu, autobusu, motoru ili bicikli. Međutim, podržani tipovi vozila variraju čime dolazi do pogrešne identifikacije, nerijetko zamjenom SUV-a s kamionom te bicikla s motorom i obrnuto. Iako je vrstu vozila relativno lako utvrditi temeljem oblika i veličine vozila, analitike korištene za prepoznavanje proizvođačke oznake ili čak modela vozila obično su prisutne kod dubokog učenja u svrhe automatskog prepoznavanja registarskih oznaka (LPR/ANPR). Takve analitike zahtijevaju znatno veći broj detalja za detekciju i samim time su složenije i skuplje. Osim za detekciju ljudi, lica i vozila, algoritmi strojnog i dubokog učenja trenirani su za detekciju i klasifikaciju naprednih objekta i njihove boje, kao što su pištolji, torbe i maske. [69]

5.2.2. Detekcija oružja

Analitika za detekciju oružja ima za cilj upozoriti nadležne organe na posjedovanje i uporabu vatrenog oružja te pomoći u pronalaženju počinitelja. Iako su algoritmi dubokog učenja trenirani na tisućama slika različitih vrsta vatrenog oružja, i ova se metoda detekcije susreće s izazovima. Mnoge predmete kao što su bušilice, mobiteli ili šalice za kavu analitika često ne razlikuje od pištolja te pošto su mnoga oružja malih dimenzija i tamne boje lako se skrivaju i teško su vidljiva na tamnoj odjeći. Na primjeru sa slike 5.6., električar često nosi bušilicu u ruci koju analitika može tumačiti kao pištolj.

Slika 5.6. Krivo tumačenje objekta [70]

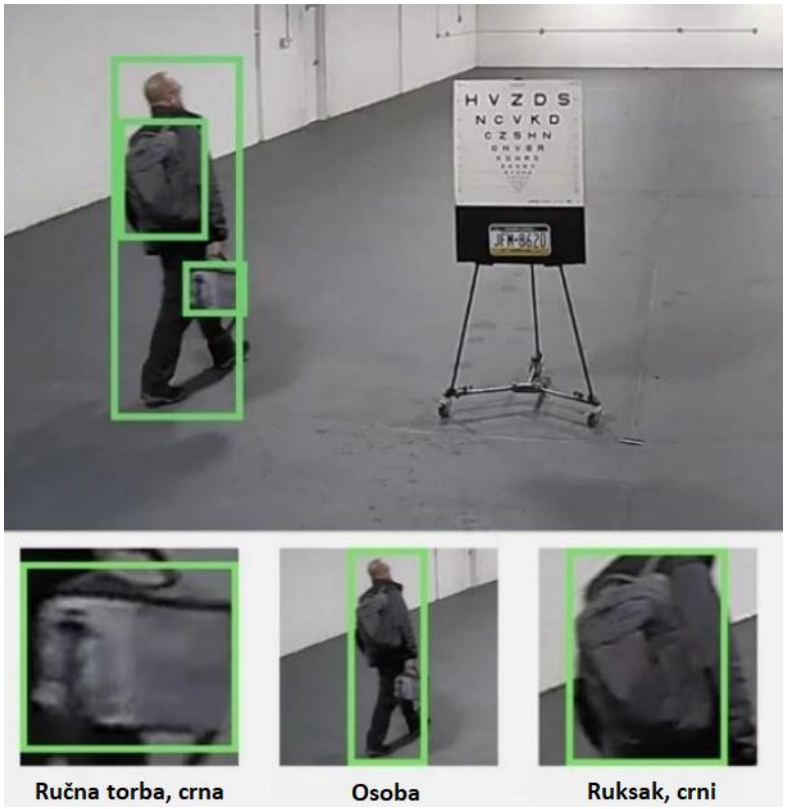
Osim toga, lažni alarmi detekcije oružja veliki su problem zbog moguće opasnosti i eventualnih skupih blokada ili zatvaranja visoko sigurnih lokacija, kao što su zračne luke, škole ili sportskih objekta.

5.2.3. Detekcija maske

Širenjem obaveze nošenja maski zbog pandemije koronavirusa, detekcija maski na licu postala je rasprostranjena u mnogim dijelovima svijeta. To je proces automatskog prepoznavanja prisutnosti maske na licu osobe na temelju analize videozapisa pomoću strojnog ili dubokog učenja. Ova vrsta detekcije proširenje je na prethodno obrađenu temu detekcije lica, gdje se nakon prvobitne detekcije samog lica pomoću specifičnog algoritma uspoređuju analizirane karakteristike s uzorcima koji predstavljaju prisutnost maske. Posebno se analiziraju glavne karakteristike lica, područje nosa, usta i brade koje maska obično pokriva te ako su pojedine karakteristike lica prisutne, većina metoda detekcije generirat će upozorenje, dok će jednostavne metode generirati alarm ako dođe do uspješne detekcije lica, što proizlazi iz činjenice da osoba ne nosi masku. Budući da jednostavna detekcija, obično algoritam strojnog učenja, „traži“ lice bez donjih karakteristika, pokrivanje tog dijela lica predmetom, kao što je mobitel, novčanice ili ruke, rezultirat će detekcijom maske na licu i slobodnom prolazu osobe. S druge strane, duboko učenje detekcije maski trenirano je na slikama ljudi koji ih nose, kako bi naučilo kako izgledaju ljudi s maskama što duboko učenje čini imunom na pokušaje prevare. Iako je detekcija maski postala posebno važna tijekom pandemije koronavirusa, primjena detekcije maski može se i dalje koristiti u zdravstvene i sigurnosne svrhe, posebno u okruženjima gdje postoji potreba za specifičnim higijenskim standardima kao što su bolnice ili industrijske postrojenja. [71]

5.2.4. Detekcija torbi

Algoritmi za detekciju torbi obično su algoritmi dubokog učenja koji se treniraju korištenjem javnih skupova podataka poput COCO-a (eng. Common Objects in Context). COCO je jedan od najpoznatijih i najraširenijih skupova podataka razvijen kako bi pomogao u istraživanju i razvoju algoritama za prepoznavanje i segmentaciju objekta u realnim scenama, što uključuje prepoznavanje objekta i njihovih odnosa u različitim okruženjima. Kao i kod drugih analitika dubokog učenja, skupovi podataka igraju ključnu ulogu u razvoju snažnih algoritama, čime se povećava njihova točnost detekcije. Na slici 5.7. prikazan je primjer uspješne detekcije i kategorizacije torbi, kao i osobe koja ih nosi.



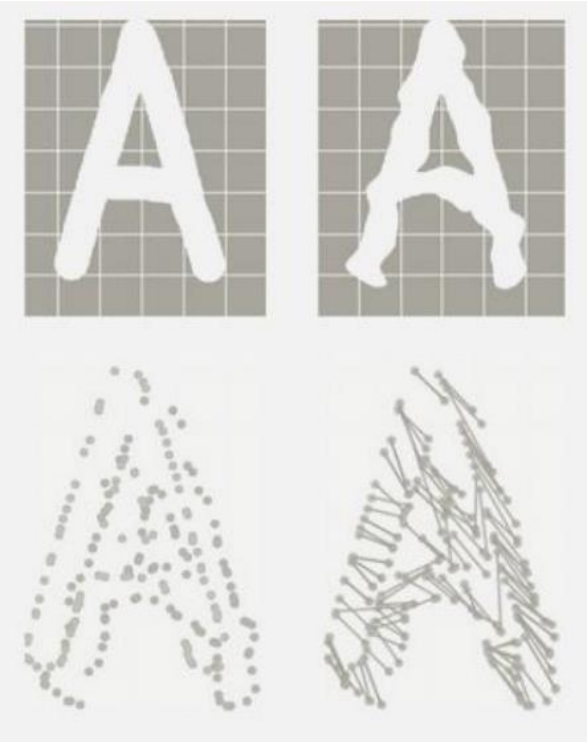
Slika 5.7. Uspješna detekcija objekata [72]

Zato što algoritam ograničava klasifikaciju isključivo uslijed prethodno detektirane osobe, što povećava vjerojatnost da je objekt torba ili ruksak, ova vrsta detekcije lagana je za klasifikaciju. Međutim, detekcija torbe kao proširenje na detekciju osoba značajno ograničava upotrebu u situacijama kada se objekt ostavi ili uzme, što je svrha za koju se detekcija torbe reklamira u kritičnim sigurnosnim aplikacijama. Objekti koji su ostavljeni ili uklonjeni su jedno od češćih pravila za detekciju torba u videonadzoru. Ova pravila ciljaju na protuterorizam ili javnu sigurnost, obično u gušćim područjima s dinamičnim osvjetljenjem, refleksijama i gotovo stalnom kretnjom.

Strojno i duboko učenje suočavaju se sa značajnim izazovima kod ovakvih objekta koji su u mnogim situacijama bezopasni. Međutim, dok je ljudima lako potvrditi istinitost je li objekt ostavljen, vrlo je teško utvrditi je li taj objekt prijetnja, čime dolazi do rizika od lažnih upozorenja je ozbiljan problem. Iako nema teoretskih ograničenja za objekte koje duboko učenje detekcije torbe može prepoznati, broj različitih objekta, kutova i svjetlosnih uvjeta nadilazi ono što se nalazi u uobičajenim skupovima podataka. Iz tog razloga, programeri su prisiljeni stvarati vlastite skupove podataka, što je skupo i teško zbog specifičnosti primjene. Također, mnogobrojna testiranja u stvarnom svijetu neophodno je provesti kako bi se analitika ispravno validirala što je u ovom slučaju teže izvedivo. Zbog tih izazova, analitika za ostavljene ili uklonjene objekte obično nije u širokoj upotrebi. [73]

5.3. Prepoznavanje tablica

Prepoznavanje registarskih oznaka ili LPR/ANPR (eng. License plate recognition/Automatic Number Plate Recognition) tehnologije su koje omogućuju automatsko prepoznavanje registarskih oznaka na vozilima. U tu svrhu koristi se kombinacija računalnog vida, optičkog čitanja i strojnog učenja kako bi se automatski detektirale registracije vozila te izdvojili alfanumerički znakovi s pločice. Računalni vid područje je u umjetnoj inteligenciji za prepoznavanje dvodimenzionalnih ili trodimenzionalnih predmeta, dok je optičko čitanje ili OCR (eng. Optical Character Recognition) tehnika koja koristi optičke senzore i računalne algoritme kako bi interpretirala vizualne podatke i prevela ih u digitalni oblik razumljiv računalu. LPR/ANPR se sastoji od dvije osnovne faze, pronalaženja tablice i čitanja znakova. Scene videonadzora mogu sadržavati brojne znakove, uključujući reklame, izloge, nazive tvrtki na vozilima itd., zbog kojih sustav prvo mora ograničiti čitanje znakova samo s registarske oznake vozila. Nakon što se pločica pronađe, izvršava se čitanje znakove s pločice koje često zna biti otežano zbog kuta gledanja kamere, veličine i fonta znakova, slika na registraciji (grb ili naljepnica), svjetline, prljavštine, vremenskih nepogoda itd. Tradicionalni OCR uzima pojedini znak s tablice kao ulazni signal te ga uspoređuje sa svim znakovima u sustavu ili ga rastavlja na dijelove i uspoređuje te dijelove s pripadajućim uzorcima. Na primjeru sa slike 5.8., slovo 'A' se stvara s jednom naglašenom linijom s lijeva na desno, jednom naglašenom linijom s desna na lijevo i jednom horizontalnom linijom. [74]



Slika 5.8. Detekcija slova „A“[75]

Pronalazeći rubove oznaka, OCR utvrđuje je li to uistinu slovo 'A'. OCR najbolje funkcionira na ravnomjerno razmaknutim i različitim znakovima jednake veličine, dok se otežano prepoznavanje dešava u slučaju velikog kuta gledanja kamere ili prekrivenih oznaka. Specifičan primjer tablica koje se u većini sustava lakše detektiraju i prepoznaju su nizozemske registarske pločice prikazane slikom 5.9.

Slika 5.9. Izgled specifične registracije [76]

One imaju visoko kontrastnu monokromatsku pozadinu sa slovima velikog fonta i dubine, veliki razmak između znakova i posebno dizajnirane znakove s urezima kako bi se bolje razlikovali slični znakovi. Najveća slabost OCR tehnike leži u sličnosti znakova, na primjer sličnost slova 'O' i 'Q' te broja '0' , slova 'I' i broja '1' te slova 'B' i broja '8' što uvelike otežava automatsko prepoznavanje oznaka. Iako je temeljnu istinu (ground truth) na registracijama koje su prepoznate relativno lako utvrditi, pločice koje su ignorirane, nisu prepoznate ili nisu otkrivene bit će potpuno propuštene.

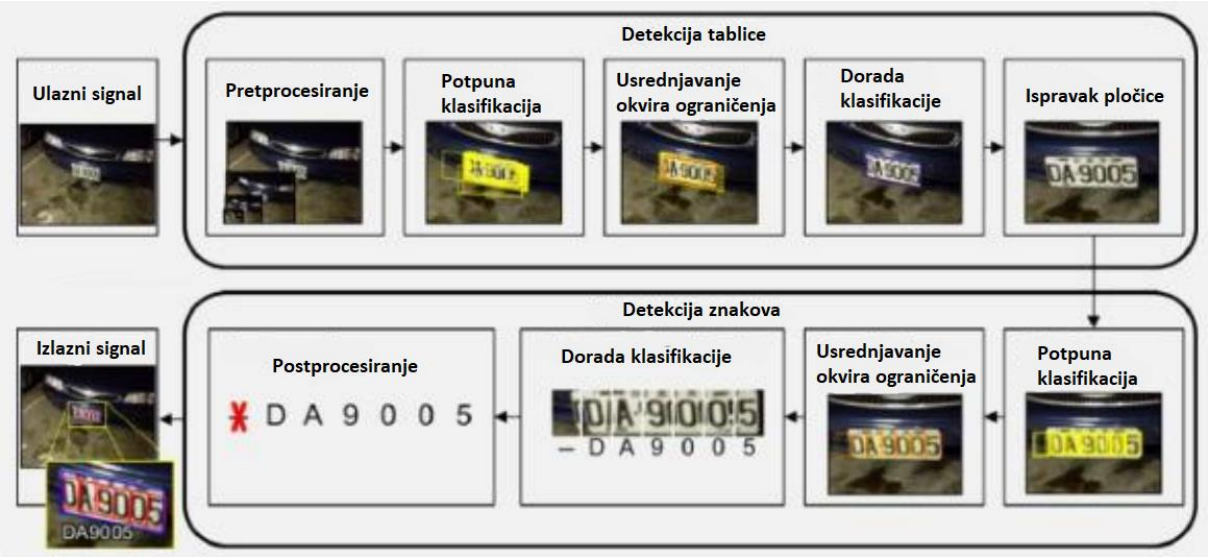
Iz tog razloga, neki LPR algoritmi imaju programiranu prilagodbu ekvivalencije kako bi se smanjilo tzv. "fuzzy" podudaranjem, tj. stopa propuštenih registarskih oznaka. Međutim, ovo povećava stopu lažnih pozitiva, što je problem usklađenosti za sigurnost i parkiranje, jer vozila s ekvivalentnim registarskim oznakama dobivaju pristup područjima za koja ne bi smjela imati pristup.

Zahtjevi za prepoznavanje registarskih oznaka u vezi s gustoćom piksela znatno variraju, ali često zahtijevaju 30-90 PPM-a što je znatno više od detekcije osoba ili vozila. Proizvođači obično specificiraju zahtjeve u pikselima prema visini ili širini pločice i/ili znakova, gdje veličina registarskih oznaka i brzina vozila značajno utječu na zahtjeve piksela, kao što je prikazano tablicom 5.1.

Tablica 5.1 Ovisnost zahtjeva piksela o veličini tablice i brzini vozila [77]

Vrsta tablice	Širina tablice[cm]	Postavljanje	Minimalna vrijednost piksela [PPM]
Američke tablice	30,5	Vozila se zaustavljaju	39
		Vozila se kreću	64,5
Europske tablice	52	Vozila se zaustavljaju	51
		Vozila se kreću	84

Iako je LPR desetljećima koristio isključivo optičko prepoznavanje znakova, razvijeni su noviji pristupi temeljeni na dubokom učenju čime je danas uobičajena hibridna kombinacija strojnog i dubokog učenja te OCR-a. Sustavi koji se temelje isključivo na dubokom učenju koriste neuronsku mrežu posebno treniranu za sustav LPR-a, dok hibridni algoritmi koriste duboko učenje za pronalaženje tablica i prilagodbu pločica na kut i osvjetljenje te zatim OCR za čitanje znakova. Proces detekcije tablice pomoću neuronske mreže dan je primjerom na slici 5.10.



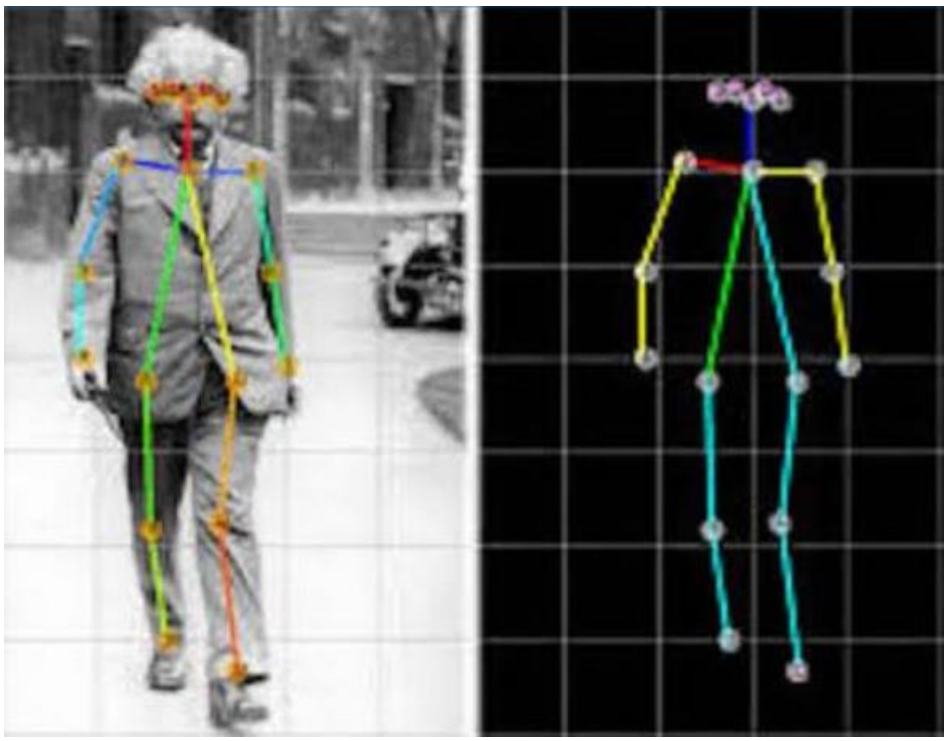
Slika 5.10. Proces detekcije tablice putem dubokog učenja [78]

Duboko učenje preciznije je i otpornije na promjene od OCR-a, bolje se nosi s mrljama i prljavštinom, osvjetljenjem i različitim kutovima gledanja, ali je pritom i značajno skuplje i zahtjevnije. Za treniranje LPR-a pomoću dubokog učenja koriste se skupovi podataka registarskih oznaka koji se u nekim zemljama redovito izmjenjuju. Takvi skupovi podataka zahtjevniji su za održavanje što otežava samo treniranje i primjenu. Za razliku od detekcija za lice, vozila i osobe, gdje je dovoljno imati do 10 fps-a, u sustavima LPR-a od velike je važnosti postići veću brzinu kadrova, minimalno 25 fps-a kako bi se mogle očitati registarske oznake s vozila u kretnji. U usporedbi s drugim tehnologijama, LPR je značajno zrelija jer je u upotrebi već mnogo godina te se često reklamira i koristi za potrebe policije, parkiranja i sigurnosti na granicama i cestama. [79]

5.4. Analiza ponašanja

Videoanalitika za analizu ponašanja tehnologija je koja koristi napredne algoritme kako bi analizirala videozapise i identificirala specifične obrasce ili aktivnosti. Glavni cilj ove analitike je razumjeti ponašanje ljudi ili objekta na temelju njihovih pokreta, pozicija ili interakcija unutar nadziranog područja. Obično se koristi za nadogradnju stvarnog nadzora, tražeći sumnjive ili nepoželjne aktivnosti (npr. neredi, tučnjave). Međutim, prepoznavanje ponašanja je teško jer vrlo različita ponašanja mogu imati slične karakteristike (npr. tučnjava, grljenje i plesanje). Ponašanja koja uključuju cijelo tijelo obično se lako potvrđuju jer većina ljudi brzo i lako može uočiti razlike između plesa, grljenja i borbenih/agresivnih ponašanja. Međutim, manje i složenije događaje, kao što su manipulacija čitačima kartica na bankomatima ili brojanje karata u kazinu, puno je teže klasificirati. Prepoznavanje ponašanja obično koristi dvije metode, a to su detekcija objekta i procjena položaja. Prepoznavanje ponašanja temeljeno na detekciji objekta koristi strojno i duboko učenje za detekciju osoba u kombinaciji s programiranim pravilima za kretanje, sudare i izgled u

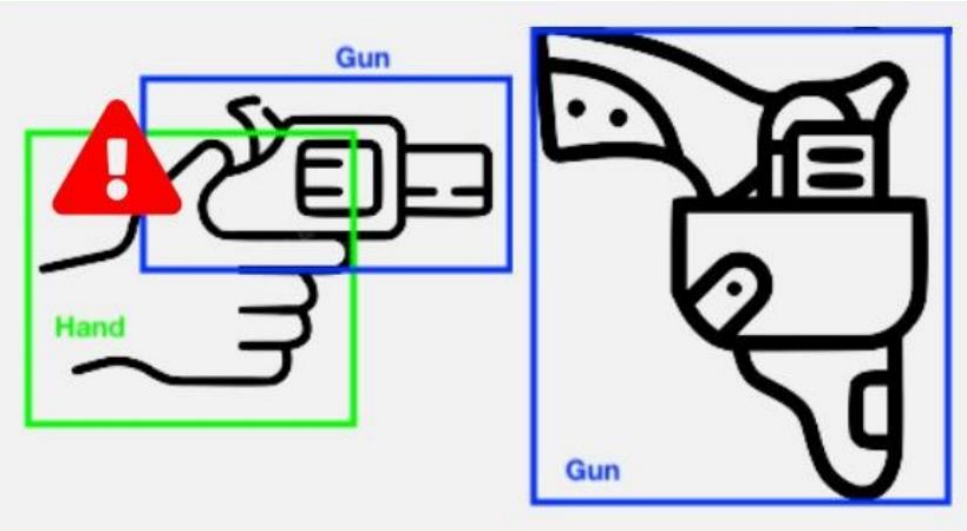
interakciji s drugim objektima (npr. oružje) radi klasifikacije ponašanja. Za procjenu položaja (eng. pose estimation) koristi se duboko učenje kako bi se stvorio kostur (eng. stick-figure) koji predstavlja čovjeka, prikazan slikom 5.11.



Slika 5.11. Stvaranje „stick-figure“-a [80]

Takav kostur koristi se za praćenje kretanja i interakcije s drugim objektima radi klasifikacije ponašanja. Procjena položaja detaljno je proučavana i često se trenira za scenarije koji nisu povezani samo s nadzorom, poput sporta gdje su subjekti uvijek ljudi pa su istraživanje i skupovi podataka relevantniji. Međutim, veliki dio snimaka dolazi s kamera postavljenih niže od visine uobičajenih nadzornih kamera, što smanjuje preciznost kada se koriste visokokvalitetne nadzorne kamere. Osim toga, procjena položaja računalno je zahtjevnija i obično zahtijeva gustoću piksela od 6-9 PPM-a, što je dva do tri puta veća gustoća piksela u usporedbi s detekcijom temeljenom na objektima.

Najčešća metoda izgradnje sustava za prepoznavanje ponašanja temelji se na pravilima definiranim od strane ljudi, koristeći procjenu položaja, detekciju objekta i druge podatke za generiranje upozorenja. Nakon što se dogodi određena aktivnost, razvijatelji analitike određuju koje su aktivnosti relevantne i koje nisu, te se ovisno o tome generira upozorenje, kao što je vidljivo se slike 5.12.



Slika 5.12. Razlikovanje opasnosti [81]

Ovakva metoda zahtijeva manje podataka za obuku koja su jasnija nego pravila definirana računalom, pri kojima će samo ranije definirana radnja pokrenuti upozorenje. Za razliku od ljudskih pravila, računala koriste označene slike i videozapise aktivnosti, zajedno s primjerima sličnih scena bez takve vrste ponašanje, za utvrđivanje optimalnog načina klasificiranja. Računala mogu optimizirati klasifikaciju znatno bolje razlikujući pokrete plesanja od pokreta tijekom tučnjave na temelju složenih odnosa između kuta koljena, brzine prema tlu i brzine prije događaja. S druge strane, pravila definirana računalom zahtijevaju puno obuke, često se loše izvode na scenama za koje nisu obučene i uče stvari koje ne bi trebale. Računalu je potrebno stotine ili tisuće pozitivnih i negativnih primjera, a lažni ili nepostojeći podaci dovode do netočnih algoritama. Iz tog razloga, prepoznavanje ponašanja podijeljeno je na nadzirane i nenadzirane metode za detekciju specifičnih i neuobičajenih ponašanja.

U većini slučajeva, obuka analitike za strojno i duboko učenje u videonadzoru provodi se nadzirano, što znači da su slike i videozapisi za obuku označeni, a računalni model odlučuje koje će karakteristike i vrijednosti koristiti za detekciju objekta. Kao što je navedeno u prethodnim poglavljima, pravilno označeni skupovi podataka su ključni za strojno učenje kako bi se ispravno detektirale aktivnosti. U nenadziranom učenju, podaci nemaju oznake te se često koristi tehnika uklanjanja pozadine, kao što je prikazano slikom 5.13.

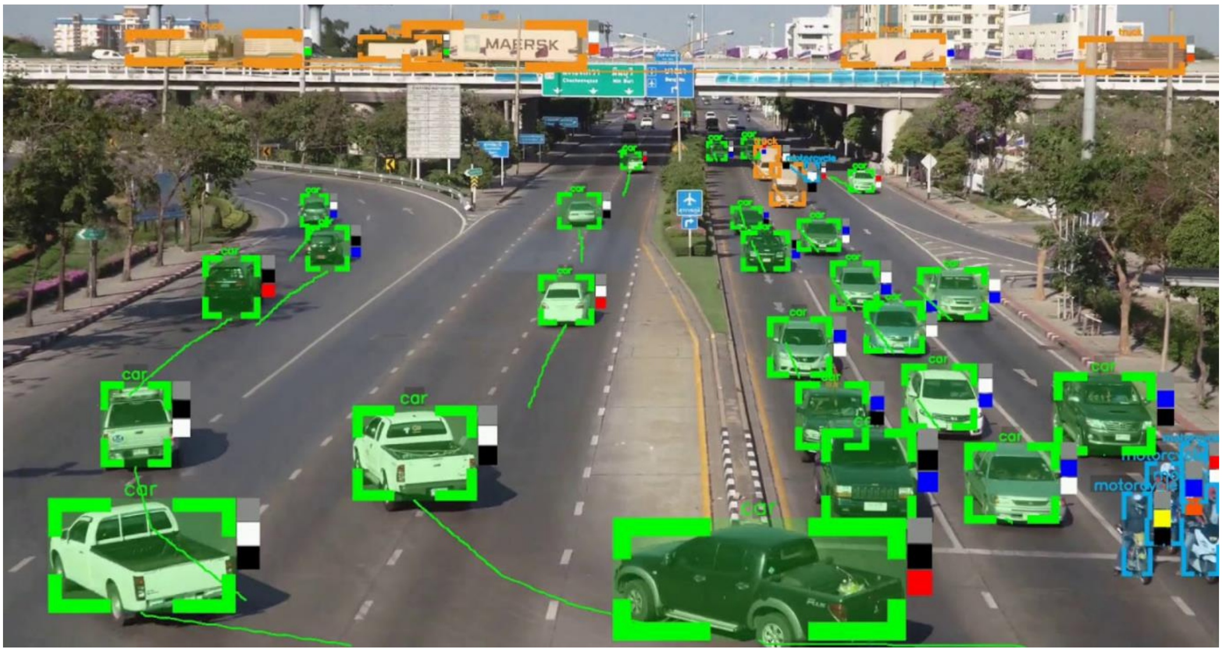
Slika 5.13. Tehnika uklanjanja pozadine slike [82]

Većina nenadziranih tehnika uklanja i analizira pozadinu scene, pošto se scena ne mijenja niti pruža nove informacije o aktivnosti. Nenadzirano učenje koristi se za obuku strojnih i dubokih modela učenja, no često radi povećanja preciznosti koristi nadzirane modele dubokog učenja za detekciju objekta. U nenadziranom učenju, algoritam koristi nepoznate podatke i sam donosi zaključke o tome što je neobično ili sumnjivo. Ovaj proces obično zahtijeva dane ili tjedne automatskog učenja da bi sustav na primjer naučio kako izgleda normalno ponašanje osobe prilikom izlaska kroz vrata. Međutim, to znači da normalno neuobičajeno ponašanje, kao što je prikupljanje smeća, nenadzirano učenje neće razlikovati od zlonamjernog neuobičajenog ponašanja, kao što je ilegalno odlaganje smeća. Isto tako, dugotrajno stajanje ispred banke može biti znak pljačke što je istovremeno i normalno ponašanje osobe koja čeka i gleda u mobitel. To također znači da će ponašanje poput tučnjave, na području gdje se često bilježe tučnjave, biti zanemareno. Budući da je neuobičajeno ponašanje ovisno o sceni, analitika mora naučiti što je normalno za svaku scenu posebno, što zahtijeva mnogo vremena. Prepoznavanje ponašanja nije tako rasprostranjeno niti temeljito istraženo kao druge analitike, a skupovi podataka većinom nisu reprezentativni za stvarne upotrebe u svijetu nadzora. Zbog toga većina razvijatelja analitike ponašanja stvara vlastite skupove podataka, često prikupljajući javno dostupne videozapise s web stranica i društvenih medija. [83]

5.5. Analiza prometa

Analiza prometa u videoanalitici proces je detaljnog proučavanja prometa vozila, pješaka ili objekata na cestama, parkinzima, trgovinama i drugim mjestima čija je svrha poboljšanje sigurnosti, učinkovitosti i upravljanja infrastrukturom. Funkcionalnosti analize prometa uključuju detekciju, praćenje i prepoznavanje objekata, brojanje vozila i pješaka, analiza brzine vozila, određivanje smjera kretnje i detekciju zagušenja na cestama. Izgled analize prometa prometnice

dan je slikom (5.14.), gdje su zelenom bojom detektirani automobili, plavom motociklisti i narančastom kamionu.



Slika 5.14. Primjer analize prometa [84]

Analiza prometa susreće sa sličnim problemima kao i prethodne vrste videoanalitike, pri kojima najveći problem predstavlja promjenjivost vremenskih uvjeta koja dovodi do lažno pozitivnih ili lažno negativnih rezultata.

5.6. Pristupi videoanalitici

Pristupi videoanalitici označavaju različite arhitekture i strategije korištene za analizu videozapisa. U sustavima IP video nadzora, takvi pristupi mogu varirati ovisno o tehničkim zahtjevima, proračunima i potrebama korisnika te se dijele na rubnu (eng. edge), centraliziranu i hibridnu videoanalitiku te videoanalitiku u oblaku. Rubna analitika podrazumijeva izvođenje analize videozapisa izravno na samoj kameri, dok se u slučaju centralizirane analitike svi videozapisi prenose i analiziraju na poslužitelju (serveru). Kombiniranjem elemenata rubne, centralizirane i cloud videoanalitike dobiva se hibridna analitika, gdje se složenija analiza odvija na serveru, snimaču ili oblaku, a jednostavnija na kameri. Cloud videoanalitika podrazumijeva proces analize videozapisa putem njegova slanja i obrade u udaljenom oblaku. [85]

5.6.1. Prednosti i nedostaci

Ovisno o primjeni , svaki od ovih pristupa sadrži razne prednosti i nedostatke prikazane tablicom 5.2.

Tablica 5.2. Prednosti i nedostaci pristupa videoanalitike [86]

Karakteristike	Rubna analitika	Centralizirana analitika	Hibridna analitika	Cloud analitika
Brzina reakcije	Brza u stvarnom vremenu	Relativno brza, ovisna o poslužitelju	Kombinira brzinu rubne i fleksibilnost centralizirane	Brza uz potrebne resurse
Kašnjenje	Nisko	Varira ovisno o mreži i poslužitelju	Ovisno je o konfiguraciji	Varira ovisno o mreži i poslužitelju
Resursi	Ograničeni na jednostavne funkcije	Niski do visoki, ovisno o poslužitelju	Kombinira rubne i centralizirane	Visoka dostupnost
Privatnost i sigurnost	Velika, podaci su lokalni	Zahtijeva posebne mjere zaštite podataka	Kombinira rubne i centralizirane mjere zaštite	Potencijalno ugrožena
Propusnost mreže	Niska	Može biti visoka, ovisna o mreži	Ovisno o konfiguraciji mreže	Visoka
Upravljanje	Zahtjevno u slučaju više uređaja	Olakšano, izvršava se s jednog mjesta	Složeno, zbog količine postavki	Omogućava udaljeno upravljanje

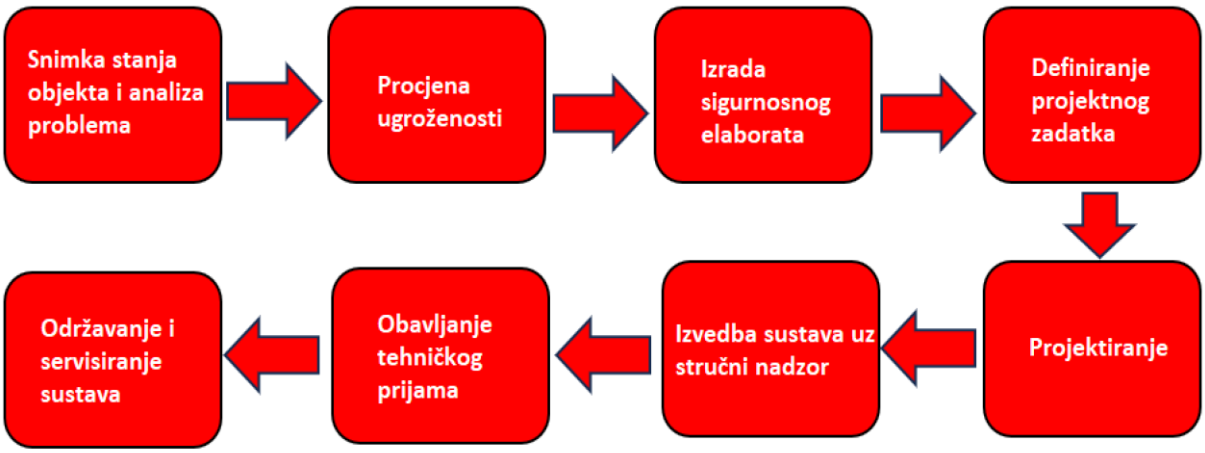
Analitika dostupna u kamerama jeftinija je opcija u odnosu na analitiku na serveru, snimaču ili oblaku, ali je pritom zbog ograničene procesorske snage kamera limitirana na detekciju pokreta, ljudi i vozila. Izuzetak su specijalne kamere koje mogu izvoditi složene videoanalitike, ali je takvim kamerama i cijena velika. U slučaju kvara kamere, ako ne postoji prenosiva licenca videoanalitike, pri zamjeni kamere potrebno je naknadno kupiti kameru s videoanalitikom što kroz vrijeme povećava troškove u odnosu na analitiku dostupnu u serveru ili oblaku, kod kojih se koriste standardne nadzorne kamere. Analitika na kameri danas se često koristi jer smanjuje potrebu za visokom propusnosti tako da kamera šalje video samo u slučaju korisnog događaja, čime se smanjuje bitrate, a time i potrebna količina pohrane.

Analitika na snimačima može pružiti najnižu cijenu po kameri jer omogućuju centralnu analizu više kamera odjednom. Uz to, umjesto zamjene kamera u svrhe dodavanja analitike, snimač može dodati analitiku postojećim kamerama. Međutim, analitika na snimaču zahtjeva i jače procesorske resurse, osobito ako se analitika treba odraditi na više kamera istovremeno što povećava ukupnu cijenu snimača. Isto tako, snimači imaju ograničeni broj kanala te ne podržavaju nadogradnje procesora, što je problematično u slučaju proširenja sustava videonadzora.

Analiza videozapisa u oblaku ima niske troškove fizičke opreme, ali skupu obradu podataka. Na ovaj način omogućava se jednostavniji pristup podacima i upozoravanje na događaje, no time se ugrožava sigurnost podataka (eng. cybersecurity) zato što videozapis mora putovati od kamere ka oblaku i natrag prema kameri. Iako videoanalitika u oblaku omogućava najsloženije analize, kao što su prepoznavanje lica i ponašanja, potrebna je velika propusnost podataka čime se može ograničiti broj kamera za analizu. Kod hibridne analitike, detekcija u kameri izvodi jednostavne zadatke, dok se resursi snimača, servera ili oblaka posvećuju složenijoj analitici čime se ostvaruje fleksibilnost analitike. Zbog složenosti integracije metapodataka između kamera i poslužitelja, ova arhitektura ograničena je na malo proizvođača te samim time visoku cijenu. Iz navedenih razloga, od velike je važnosti odabrati odgovarajuću vrstu pristupa videoanalitici ovisnu o potrebama korisnika te resursima i arhitekturi sustava videonadzora. [86]

6. PROVEDBA TEHNIČKE ZAŠTITE

Provedba tehničke zaštite delikatan je postupak zaštite određenog objekta čiji je procesni tok dan slikom 6.1.

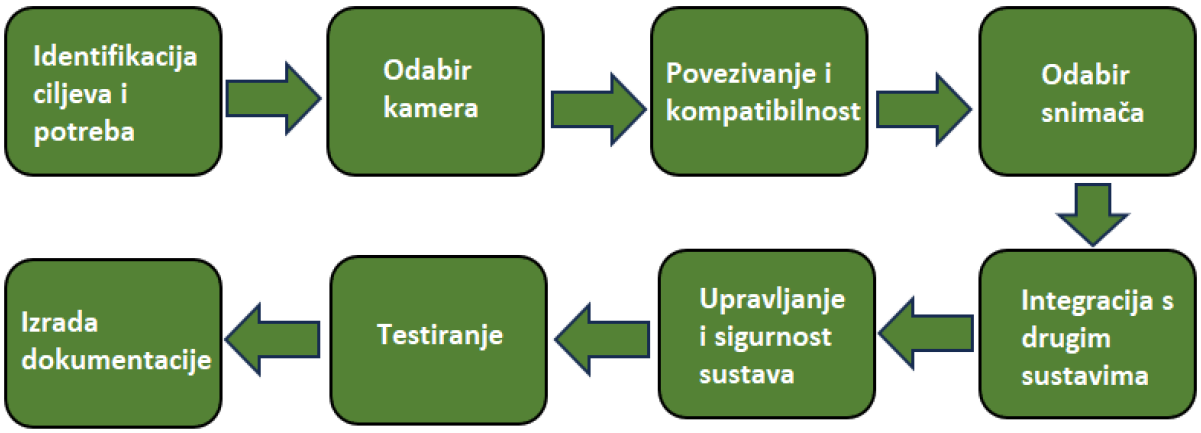


Slika 6.1. Proces izvedbe tehničke zaštite

Proces započinje snimanjem postojećeg stanja štićenog objekta i analizom uočenih problema na objektu. Slijedi izrada prosudbe ugroženosti koja identificira potencijalne prijetnje i slabosti objekta te pomaže u donošenju odluka o sigurnosnim mjerama opisanim u sigurnosnom elaboratu. Nakon toga, definira se projektni zadatak u kojem se određuje koje sustave treba projektirati kako bi se objekt adekvatno zaštitio. Projektiranje određenog zadatka ovisi o sustavu zaštite koji se primjenjuje na objekt te se sastoji od mnogo koraka koji će detaljno biti opisani u nastavku. Po završetku projektiranja provodi se izvedba sustava tehničke zaštite koja predstavlja fizičku implementaciju svih elemenata, uređaja i mjera definiranih u projektnom zadatku. Ovaj proces uključuje postavljanje opreme, konfiguraciju sustava i testiranje funkcionalnosti uz prisutnost stručnog nadzora. Stručni nadzor osigurava koordinaciju između radnika na objektu te provjerava je li odrađena implementacija u skladu s tehničkim planom, specifikacijama i standardima. Obavljanje tehničkog prijama sustava tehničke zaštite je faza koja dolazi nakon izvedbe i instalacije sigurnosnih mjera. Ovaj postupak uključuje provjeru ispravnosti, funkcionalnosti i usklađenosti sustava s planom, specifikacijama te zahtjevima i očekivanjima naručitelja ili vlasnika objekta. Ako je sustav po svim aspektima ispravan, pušta se u rad sve dok ne dođe do problema koje treba servisirati ili do trenutka kada je potrebno odraditi redovno održavanje sustava.

6.1. Projektiranje sustava videonadzora

Projektiranje sustava videonadzora proces je koji zahtijeva pažljivo planiranje, analizu potreba korisnika i odabir odgovarajuće opreme. Kao što je prikazano slikom 6.2., proces započinje identifikacijom ciljeva i potreba nadzora, tj. koja područja kamere trebaju pokrivati i koje vrste događaja je nužno pratiti i bilježiti.



Slika 6.2. Proces projektiranja

Ovisno o potrebama, odabire se vrsta, broj i pozicija kamera na objektu u svrhe ostvarenja optimalnog nadzora. Nužno je predvidjeti način na koji će se kamere i ostali uređaji povezati na mrežu odabirom optimalnog mrežnog preklopnika te duljine i vrste kabela kao i kompatibilnost s određenim standardima i protokolima. Isto tako, ako se koristi postojeća mreža potrebno je s IT službom provjeriti propusnost mreže kako videonadzor ne bi narušio poslovnu aktivnost objekta. U odnosu na broj kamera, kvalitetu slike i metodu kompresije video sadržaja neophodno je predvidjeti potrebnu veličinu pohrane i broj kanala mrežnog video snimača. Također, bitno je uzeti u obzir i eventualnu potrebu integracije s drugim sustavima kao što su alarmni sustavi ili kontrola pristupa u svrhe dodatne zaštite objekta. Planira se kako će korisnik/osoblje upravljati i pratiti sustav, tko će sve imati pristup određenom video sadržaju te kako će se postupati u slučaju alarma ili detekcije sumnjivih radnji. Po završetku projekta, izrađuje se dokumentacija/troškovnik koja sadrži tehničke specifikacije, crteže postavljanja kamera te ukupnu i pojedinačnu cijenu elemenata i utrošenih sati rada radnika.

7. PROJEKT

S obzirom na sva do sad obrađena poglavlja, opisat će se primjer projektiranja prometnog raskršća kao i sve što je potrebno kako bi se uspješno realizirao jedan takav projekt. Prvo je potrebno posjetiti zadanu lokaciju uz prisustvo nadležne osobe investitora kako bi se utvrdile pojedinosti vezane za područja koja se žele snimati, u ovom slučaju raskršće i svi prilazi. Osim želje za nadzorom, potrebno je ostvariti brojanje vozila i prepoznavanje tipa i registracije vozila uz pohranu podataka u trajanju od 30 dana kroz svih 24 sata u danu. U te svrhe, uzeti će se četiri kamere marke Vivotek, od kojih su tri Box kamere u kućištu za vanjsku ugradnju s ugrađenim IR reflektorom, a četvrta je širokokutna Dome kamera, prikazanih slikom 7.1.

Slika 7.1. Kamere korištene na lokaciji [87]

Na Box kamerama nalazi se analitika za prepoznavanje registarskih pločica i vrste vozila, dok je na Dome kameri ugrađena videoanalitika koja može brojati prolaske vozila kroz raskršće iz svih smjerova. Osim kamera, na nacrtu je potrebno ucrtati trase po kojima će se provlačiti instalacije sve do određene točke gdje se nalazi vanjski ormar s mrežnim preklopnikom. Navedeni ormar se optičkim kabelom povezuje s centralnom lokacijom gdje će se videonadzor obrađivati i pohranjivati. Za povezivanje sa strane ormara koristi se industrijski mrežni preklopnik, dizajniran za rad pri većem temperaturnom rasponu u odnosu na standardne preklopnike, koji sadrži utore za optičke priključke ili SFP (eng. Small Form-factor Pluggable) brzine do 1 Gbps, dok se na strani centralne lokacije nalazi mrežni preklopnik koji također sadrži SFP utore. Izuzev optičkih portova, odabrani industrijski preklopnik ima 6 portova brzine do 100 Mbps za mrežno povezivanje s kamerama, od kojih su četiri porta predviđena za kamere, a dva su rezerva za potencijalno proširivanje sustava ili se želi upravljati preklopnikom s prijenosnim računalom na samoj lokaciji. Zbog potreba za napajanjem i komunikacijom kamera, vanjska instalacija sastoji se od PP/J 3x1,5

mm^2 napajačkog kabela i FTPcat7 Outdoor kabela za komunikaciju. Duljine pojedinačnog mrežnog kabela u ovom slučaju ne premašuju 100 metara čime se osiguralo potpuno očuvanje signala. Zato što su sastavni dio ovih kamera IR reflektor i vanjsko kućište, koje se sastoji od grijača i ventilatora, veliki potrošači struje, potrebno je kamere spojiti na 24VDC napajač koji se nalazi u vanjskom ormaru. Za snimač je odabran server sa specijalističkom programskom aplikacijom koja osim snimanja video sadržaja omogućuje i analizu podataka dobivene iz videoanalitike kamere. Kamera prema snimaču uz videozapis šalje i metapodatke iz videoanalitike, gdje se u programskoj aplikaciji obrađuju metapodaci i pohranjuju u bazu podataka registracija i vrste vozila. Za arhiviranje podataka nužno je odabrati optimalnu veličinu tvrdog diska ovisnu o brzini prijenosa podataka, broju kamera i periodu snimanja. Box kamere imaju Full HD razlučivost slike, dok Dome kamera ima 8 Mpx (4k) razlučivost uz H.265 kompresiju videa i 20 fps-a. Izvučeno iz deklariranih podataka proizvođača, veličina jedne komprimirane slike iznosi 45 kB, čime se pomoću formule (4.2.) dobiva iznos bitrate-a:

$$Bitrate = veličina\ komprimirane\ slike\ [kB] \cdot brzina\ kadra\ \left[\frac{broj\ slika}{s}\right] = 45 \cdot 20$$
$$= 900\ \left[\frac{KB}{s}\right] = 900 \cdot 8 = 7200\left[\frac{kb}{s}\right] = 7{,}2\left[\frac{Mb}{s}\right]. \qquad (6.1)$$

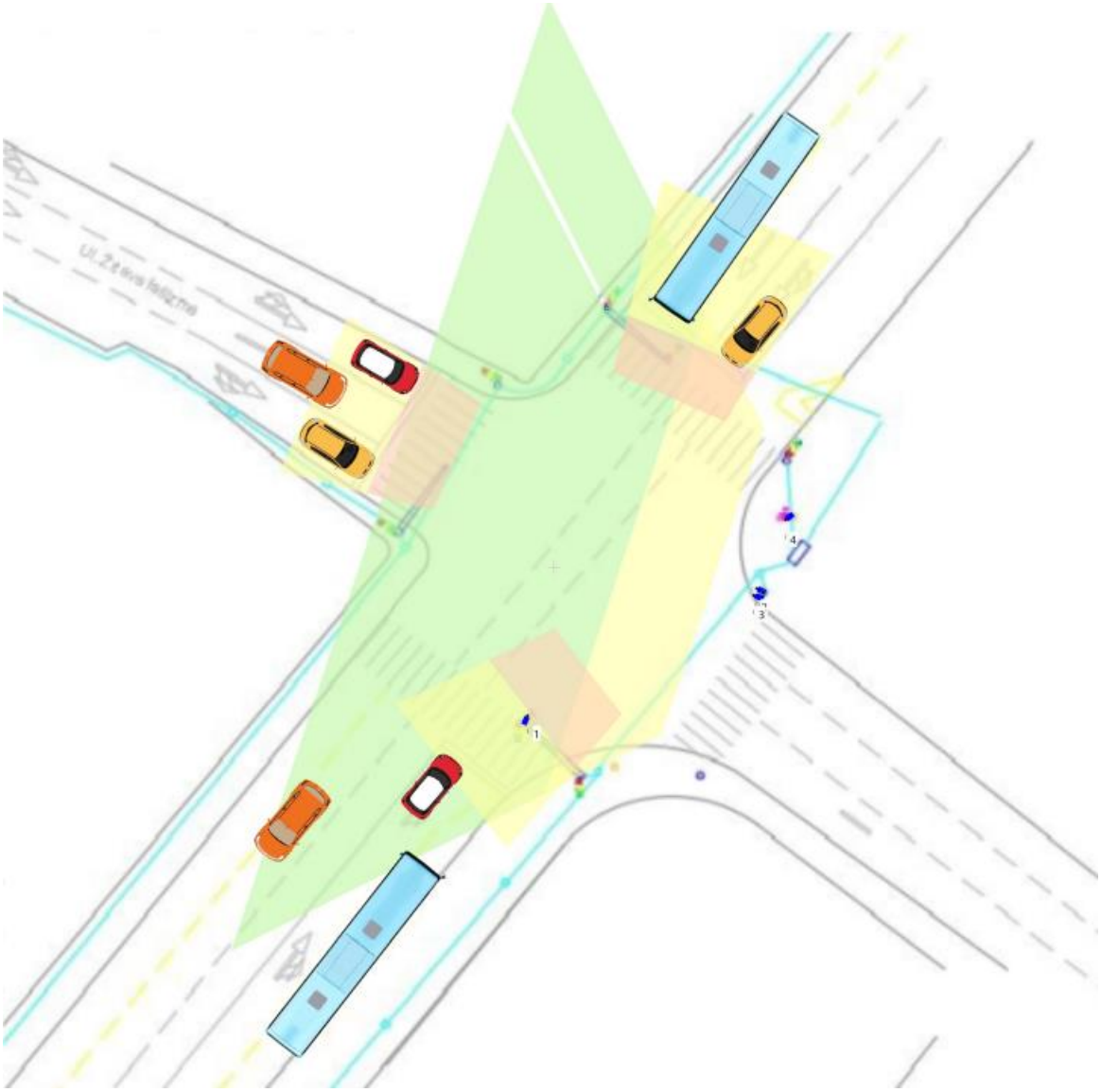
Nakon što se dobije iznos brzine prijenosa podataka, potrebno je odrediti minimalnu potrebnu memoriju tvrdog diska. Za ovaj slučaj uzeti će se 4 kamere koje snimaju cjelodnevno te se snimke pohranjuju tijekom 30 dana nakon kojega se brišu. Nakon uvrštavanja u jednadžbu:

$$Ukupna\ memorija = broj\ kamera \cdot bitrate\left[\frac{mb}{s}\right] \cdot vrijeme[s], \quad (6.2)$$

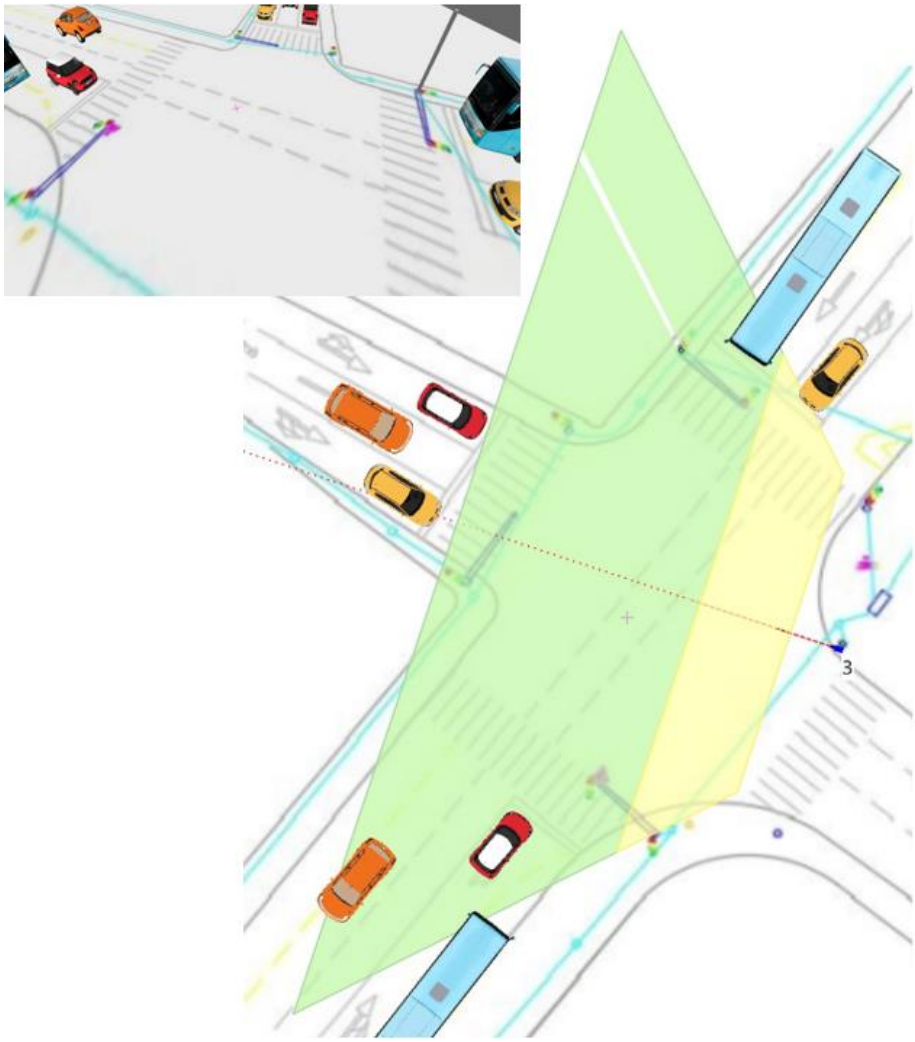
dobiva se:

$$Ukupna\ memorija = 4 \cdot 7{,}2 \cdot 30 \cdot 24 \cdot 3600 = 74649600\ [mb] = \frac{74649600}{8}$$
$$= 9331200[MB] = \frac{9331200}{1024 \cdot 1024} = 9.11[TB]. \qquad (6.3)$$

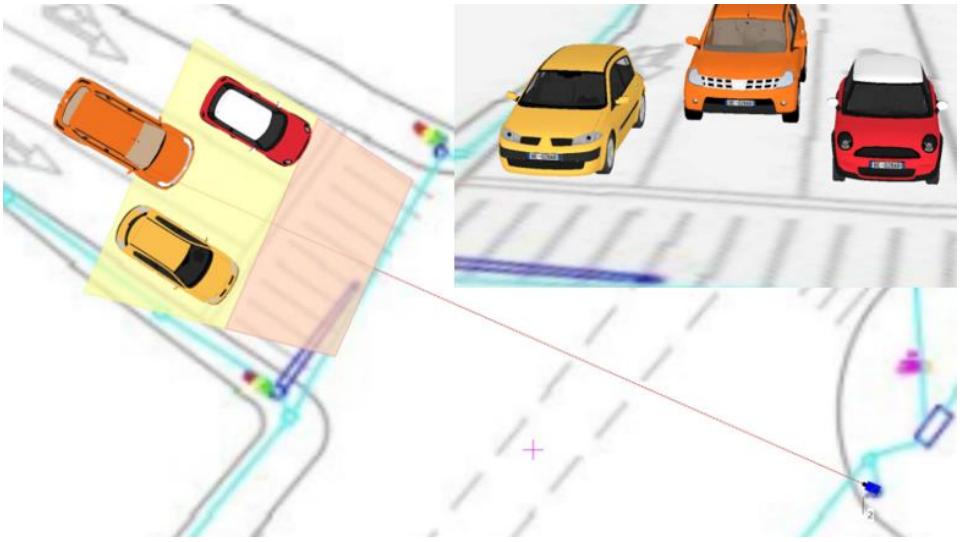
Prilikom odabira adekvatne veličine tvrdog diska, iznos pohrane podataka dobiven izračunom uvijek se uvećava za 20% zbog mjere pogreške do koje dolazi uslijed promjenjivosti parametara unutar sustava videonadzora. S obzirom na to da je projekt videonadzora poslovna tajna, primjer projekta prikazan je slikama 7.2., 7.3. i 7.4., gdje su priloženi nacrti izrađeni u programskom paketu VSDT (eng. *Video System Design Tool*) te se ne odnosi na stvarnu lokaciju.



Slika 7.2. Prikaz raskršća u VSDT-u



Slika 7.3. Prikaz raskrižja iz pogleda Dome kamere



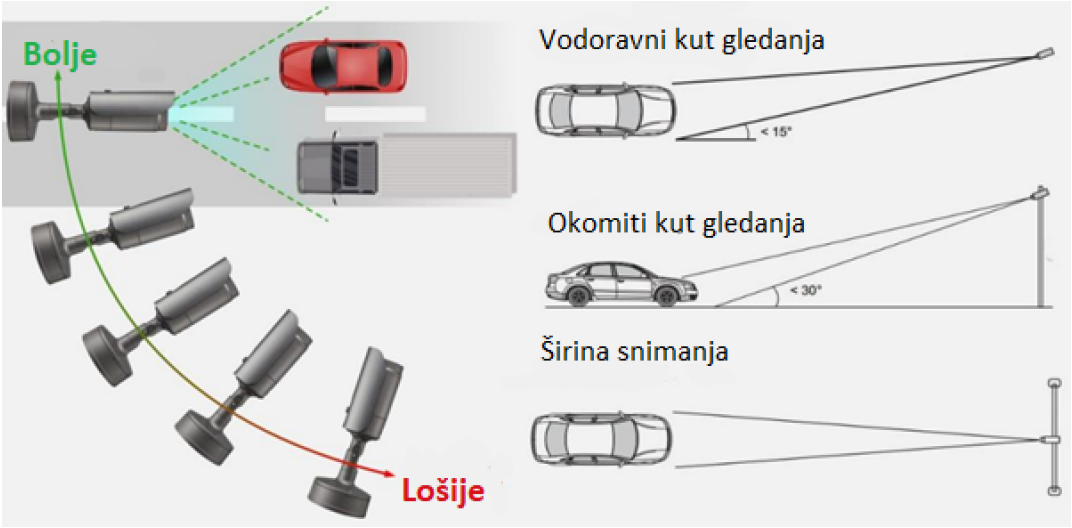
Slika 7.4. Prikaz raskrižja iz pogleda jedne Box kamere

Pomoću ovog programskog paketa moguće je i simulirati prikaz svake kamere uz odabrane parametre što je korisno za provjeru željene funkcionalnosti, vidljivo sa slika 7.5. i 7.6.

Slika 7.5. Simulirani prikaz Dome kamere

Slika 7.6. Simulirani prikaz Box kamere

Kamere se ugrađuju na povišene pozicije kao što su rasvjetni stupovi ili konzole semafora tako da što direktnije gledaju vozila iz određenog smjera. Za razliku od Dome kamera, koje za brojanje prometa zahtijevaju veliko vidno polje za pokrivanje što većeg dijela raskršća, Box kamere za prepoznavanje tablica moraju imati usko vidno polje i biti precizno orijentirane i nagnute, kao što je prikazano slikom 7.7.



Slika 7.7. Pozicioniranje kamera [88]

Zbog toga što se u ovom slučaju Box kamere koriste i za prepoznavanje tipa vozila, vidno polje je potrebno povećati, ali ne previše kako bi se mogle ispravno prepoznavati i registarske oznake. Po završetku projektiranja izrađuje se troškovnik sa svom potrebom opremom i radovima u obliku „Excel“ tablice. U troškovniku se specificiraju karakteristike kamera i snimača za traženu funkcionalnost uz procjenu ulaganja kako bi investitor ima uvid u cijenu takvog sustava, a primjer troškovnika dan je u nastavku.

TROŠKOVNIK

R.br.	Opis	Jedinica mjere	Količina
	Oprema i radovi		
1	Dobava, isporuka, ugradnja i spajanje mrežne kamere sljedećih minimalnih traženih karakteristika: - LPR kamera s ugrađenim softverom za prepoznavanje tablica automobila više zemalja (min. europske zemlje) i tipa vozila - u kompletu s kućištem, s vanjskim IR reflektorom - razlučivost min. 2Mpx (min. 1920 x 1080), min. 50fps ili bolje - domet reflektora minimalno 30 m, daljinsko podešavanje kuta reflektora - kompresija H.265/H.264/MJPEG - motorizirani objektiv min. raspona 12-40mm ili više, daljinsko podešavanje fokusa - mogućnost prepoznavanja registracije za brzine automobila minimalno 80 km/h ili više - istovremeno prepoznavanje u dvije ili više voznih traka - min. sljedeće funkcije Dan/Noć, WDR (široki dinamički raspon), 3DNR (3D kompenzacija šuma), HLC (kompenzacija farova automobila) - WDR 140 dB ili više - elektronička stabilizacija slike (DIS), defog funkcija - napajanje 24Vac/dc ili PoE+ ili drugo - min broj ulaza/izlaza 2/2, RS485 komunikacija - IP68, IK10 ili bolja zaštita kućišta - ugrađena zaštita od kibernetičkih napada	kom	3

2	Dobava, isporuka, ugradnja i spajanje mrežne kamere s ugrađenom prometnom analitikom: - vanjska antivandal dome kamera - razlučivost min 8Mpx (min 3840x2160 piksela), min 25fps ili bolje - kompresija H.265/H.264/MJPEG, - motorizirani objektiv minimalno raspona f4-10mm ili više, daljinsko podešavanje fokusa - vodoravni kut vidnog polja min. 100 st. ili više - min. sljedeće funkcije Dan/Noć, NV, WDR, 3DNR, - operativni sustav koji omogućuje ugradnju više tipova video analitike za analizu prometa - IR domet min. 50m ili više - napajanje 24Vac/dc ili PoE+ ili drugo - IP67, IK10, NEMA4X ili bolja zaštita kućišta - radna temperatura minimalno u rasponu od -30ºC do +60ºC ili večem	kom	1
3	Dobava, isporuka i ugradnja odgovarajućeg nosača za stup za mrežne kamere	kom	3
4	Dobava, montaža, spajanje, programiranje upravljivog industrijskog PoE+ mrežnog preklopnika u kućištu za vanjsku montažu - predviđen za rad u vanjskim uvjetima - min. 6x 100Mbps Rj45 + 1x 1Gbps SFP priključaka - min 60W na PoE priključku - radna temperatura minimalno u rasponu od -30°C do 60°C ili više - u potpunosti upravljiv putem mrežnog sučelja ili konzolnog priključka, mogućnost podešavanja VLAN-ova	kom	1
5	Dobava, isporuka, ugradnja i spajanje SFP gigabitnog modula za spajanje singlemodnog svjetlovodnog kabela na mrežni preklopnik kategorije 1000BASE-SX - industrijski, za vanjske uvjete	kom	2
6	Komplet za spajanje 4 niti optičkog kabela - kazeta - pigtail - zavarivanje kabela	kom	2
7	Dobava, isporuka, polaganje i uvlačenje optičkog kabela s minimalno 4 niti za vanjsko polaganje u kabelske police i/ili DTK i/ili plastične tvrde samogasive cijevi, komplet s označavanjem i svim potrebnim radovima i pomoćnim materijalom:	m	350
8	Dobava, isporuka, polaganje i uvlačenje signalnog kabela: S/FTP cat.7.	m	300
9	Dobava, isporuka, polaganje napojnog kabela komplet sa spajanjem, označavanjem i svim potrebnim radovima i pomoćnim materijalom: NYY-J 3x1,5mm^2.	m	150
10	Ispitivanje ispravnosti ožičenja izvedene FO i S-FTP mrežne infrastrukture te propisana mjerenja	kpl	1
11	Dobava, isporuka, ugradnja i spajanje poslužitelja sustava videonadzora slijedeće tehničke karakteristike: • Intel Core i7 procesor / min 3,06 GHz, 8 MB, 1066 Mhz ili bolje • 2x 8GB DDR4 Memorija • matična ploča: podrška za i7 procesor, DDR4 radne memorije, • hard disk: SSD 256 GB + 2x HDD 8TB • dodatna grafička kartica: s grafičkim procesorom, clock>1000MHz i min. 4GB RAM-a, brzina memorije min.7Gbps • 2 x mrežna kartica: 1 x 10/100/1000 • USB tipkovnica, USB Opticki scroll miš, • kućište: minitower • Microsoft Windows 10 Pro 64 • antivirusni program.	kom	1

12	Dobava, isporuka, instalacija i podešavanje serverske aplikacije s 4 licence za kamere- snimanje, pregled zapisa- prikaz podataka iz video analitike uključivo prepoznavanje tablica- prikaz statistike brojanja vozila	kom	1
13	Dobava, isporuka i ugradnja uređaja za besprekidno napajanje minimalnih tehničkih karakteristika: • Vrijeme rada pod opterećenjem od 1000W: min 20minuta ili više • Kapacitet izlazne snage: 3000/2700 (VA/W) ili više • Nominalni ulazni napon 200-276V • Frekvencija : 50/60 Hz	kom	1
14	Dobava i montaža rack ormara 15U - uključene polica, horizontalne vodilice, 24 portni prespojni panel RJ45, napojna letva u rack izvedbi	kom	1
15	Podešavanje i programiranje parametara rada računala sustava videonadzora s unošenjem korisničkih podataka.	kom	1
16	Dobava, isporuka, ugradnja i spajanje prespojnih (patch) kabela cat6 dužine 2m za vezu između portova prespojnih panela i portova komunikacijske opreme	kom	4
17	Dobava, isporuka i spajanje prespojnih FO SM 9/125µm kabela: - patch kabel LC - LC duplex l=2m	kom	2
18	Dobava, isporuka, ugradnja i spajanje mrežnog preklopnika sljedećih minimalnih karakteristika: - min 4-Portova 100Mbps RJ45 +1-Port 1Gbps SFP ili više - upravljanje putem web sučelja, mogućnost podešavanja VLAN-ova	kom	1
19	Programiranje rada mrežnih preklopnika, konfiguracija IP adresa i podešavanje sigurnosti na portovima.	kompl	1
20	Izrada pisanih uputa za rukovanje i održavanje sustava videonadzornog sustava.	kpl	1
21	Obuka korisnika za rukovanje sustavom videonadzora	kpl	1
22	Primopredaja sustava korisniku s kompletnom programskom dokumentacijom.	kpl	1
23	Izrada projekta izvedenog stanja	kpl	1

8. ZAKLJUČAK

Razvoj IP sustava videonadzora neprestano napreduje kako bi se zadovoljile rastuće potrebe sigurnosti i efikasnosti u današnjem dinamičnom okruženju. Pravilna konfiguracija fizičkih i programskih komponenti, integracija s drugim tehnologijama i adekvatno upravljanje od velike su važnosti pri ostvarivanju punog potencijala sustava. Suočeni s dinamičnim zahtjevima u pogledu sigurnosti i nadzora, projektiranje sustava videonadzora postaje ključna komponenta osiguranja učinkovite zaštite i praćenja događaja. Zaključno s troškovnikom, jasno je vidljivo kako je projektiranje složeni proces gdje presudnu uloga igra usklađivanje sa specifičnim potrebama određenog okruženja. Iz tog razloga, valja imati na umu da praktična primjena uvijek donosi i izazove, gdje upravljanje velikim količinama podataka, zaštita privatnosti, održavanje sustava i osiguranje kontinuirane operabilnosti zahtijevaju pažnju i stručnost. Isto tako, bitno je detaljno poznavati svaku komponentu sustava, od dijelova i načina rada pa sve do prednosti i nedostataka varijante svake komponente u svrhe odabire optimalne za pojedinu situaciju. Osim toga, videoanalitika unutar IP sustava videonadzora prekretnica je u načinu na koji se promatra i primjenjuje nadzor u različitim kontekstima, čime ova tehnologija omogućuje dublju i dinamičniju analizu podataka, pružajući prijeko potrebne informacije i uvide za bolje donošenje odluka. Međutim, kako se ova tehnologija sve više integrira u svakodnevni život, dolazi do sve češćih pitanja privatnosti, pouzdanosti algoritama i etičke dileme čime se narušava ravnoteža između napretka i odgovornosti. Budućnost IP sustava videonadzora obećava sve inteligentnija i prilagodljivija rješenja za sigurnost i nadzor gdje kritična suradnja između tehnologije, etičkih smjernica i individualnih prava igra ključnu ulogu u osiguravanju da ove inovacije doprinesu stvarnoj dobrobiti društva, uz istodobno poštivanje osnovnih vrijednosti sigurnosti i privatnosti.

LITERATURA

[1] IPVM: “2023 Video Surveillance”, pp. 1-14

[2] Internetska stranica (pristupljeno 15.08.2023.): https://www.itgovernance.co.uk/blog/does-your-use-of-cctv-comply-with-the-gdpr

[3] Internetska stranica (pristupljeno 13.07.2023.): https://www.researchgate.net/profile/Pooya-Zanjani/publication/259931395/figure/fig5/AS:668359112785930@1536360638637/Internal-components-of-a-network-camera.ppm

[4] Internetska stranica (pristupljeno 14.07.2023.): https://www.ipphone-warehouse.com/blog/ip-camera-image-sensor-guide-ccd-cmos

[5] Vivotek inc.: “VEC Training Course Modelu 4 – Front End Technology“, 2013.

[6] Nakamura J.:"Image Sensors and Signal Processing for Digital Still Cameras", 2006.

[7] Internetska stranica (pristupljeno 20.07.2023.): https://www.conrad.hr/p/vivotek-objektiv-al-242-vivotek-al-242-2108986

[8] Vivotek inc.: “VEC Training Course Modelu 4 – Front End Technology“, 2013.

[9] Internetska stranica (pristupljeno 10.07.2023.): https://www.bhphotovideo.com/explora/photography/buying-guide/understanding-camera-lenses

[10] Internetska stranica (pristupljeno 15.08.2023.):

[11-14] Vivotek inc.: “VEC Training Course Modelu 4 – Front End Technology“, 2013.

[15] Kuhn A.:"The Camera", 2012.

[16] Internetska stranica (pristupljeno 21.07.2023.): https://hr.technology-news-hub.com/2731-what-is-aperture

[17] Internetska stranica (pristupljeno 10.07.2023.): https://www.fot-o-grafiti.hr/nauci/op%C4%87e-osnove/f-broj

[18] March Networks: „Understanding IP Camera Features – Depth of Field“, 2016.

[19] Vivotek inc.: “VEC Training Course Modelu 4 – Front End Technology“, 2013.

[20] Internetska stranica (pristupljeno 10.07.2023.): https://hr.wikipedia.org/wiki/Ogib

[21] Schumachera-Rasmussena E.:"Digital Video Essentials: Shoot, Transfer, Edit, Share", 2005

[22-26] Vivotek inc.: “VEC Training Course Modelu 4 – Front End Technology“, 2013.

[27] Internetska stranica (pristupljeno 14.07.2023.): https://www.birddogdistributing.com/color-temperature-scale/

[28] Vivotek inc.: “VEC Training Course Modelu 4 – Front End Technology“, 2013.

[29] Internetska stranica (pristupljeno 18.07.2023.): https://en.wiktionary.org/wiki/RGB

[30] Vivotek inc.: “VEC Training Course Modelu 4 – Front End Technology“, 2013.

[31] Vivotek inc.: “VEC Training Course Modelu 4 – Front End Technology“, 2013.

[32] Kruegle H.: "CCTV Surveillance: Analog and Digital Video Practices and Technology", 2010.

[33-36] Internetska stranica (pristupljeno 10.08.2023.): https://www.vivotek.com/

[37] Internetska stranica (pristupljeno 10.08.2023.): https://www.firelab.org/resource/thermal-imaging

[38] Internetska stranica (pristupljeno 12.08.2023.): https://www.hikvision.com/en/products/IP-Products/Network-Video-Recorders/

[39] Chuvakin, A., Newman, D.: ”Network Video Recorder (NVR) Security”, 2015.

[40] IPVM: “2023 Video Surveillance”, pp. 27-50

[41] A. Murat Tekalp: “Digital Video Processing”, 1995.

[42] Internetska stranica (pristupljeno 12.07.2023.): https://www.epiphan.com/blog/h264-vs-h265

[43] IPVM: “2023 Video Surveillance”, pp. 27-50

[44] Internetska stranica (pristupljeno 25.07.2023.): https://en.wikipedia.org/wiki/Coaxial_cable

[45] Internetska stranica (pristupljeno 25.07.2023.): https://www.techtarget.com/searchnetworking/definition/coaxial-cable-illustrated

[46] Internetska stranica (pristupljeno 25.07.2023.): https://shop.kerman.hr/Katalog/Detalj/405?Konektor-BNC/F

[47] Internetska stranica (pristupljeno 25.07.2023.): https://www.wenchangcable.com/news/what-is-utp-ftp-sftp-network-cable

[48] Internetska stranica (pristupljeno 25.07.2023.): https://www.universalnetworks.co.uk/faq/what-does-utp-s-utp-ftp-stp-and-sftp-mean/

[49, 50] Internetska stranica (pristupljeno 25.07.2023.): https://community.fs.com/blog/patch-cable-vs-crossover-cable.html

[51] Internetska stranica (pristupljeno 25.07.2023.): https://stl.tech/blog/what-is-a-utp-cable/

[52] Internetska stranica (pristupljeno 25.07.2023.): https://www.teslacables.com/proizvod/377

[53] Khare R.P.: "Fiber Optic Essentials", Oxford Univ., 2004.

[54] Internetska stranica (pristupljeno 26.07.2023.): http://hr.fttxsolution.com/fiber-connectors/sc-fiber-connectors/sc-pc-fiber-connectors.html

[55] Internetska stranica (pristupljeno 26.07.2023.): https://www.fs.com/de-en/products/12085.html

[56] Shanmugavadivu, P. D., Kumar, K. S.: „A review of video surveillance systems and technologies“, International Journal of Scientific & Engineering Research, 2016.

[57] Internetska stranica (pristupljeno 27.07.2023.): https://www.tp-link.com/us/business-networking/solution/switches-for-surveillance/

[58] Anixter:"IP Video Surveillance: A Guide to Planning, Deploying, and Managing IP Video Solutions", 2015.

[59] Abbas, T. K., & Shehzad, K.: „A comparative study of managed and unmanaged network switches for small and medium enterprises“, International Journal of Computer Science and Information Security, 2016.

[60] B. Han et al.: "A Survey of Video Analytics in the Cloud", 2019.

[61-64] IPVM: “2023 Video Analytics”, pp. 1-22

[65-73] IPVM: “2023 Video Analytics”, pp. 72-89

[74-79] IPVM: “2023 Video Analytics”, pp. 137-157

[80-83] IPVM: “2023 Video Analytics”, pp. 89-117

[84] Internetska stranica (pristupljeno 30.07.2023.): http://www.goodvisionlive.com

[85] IPVM: “2023 Video Analytics”, pp. 22-41

[86] IPVM: “2023 Video Analytics”, pp. 22-41

[87] Internetska stranica (pristupljeno 20.08.2023.): https://www.vivotek.com/products/network-cameras

[88] IPVM: “2023 Video Analytics”, pp. 22-41

POPIS SLIKA

POPIS TABLICA

POPIS KRATICA I OZNAKA

IP	Internetski protokol (eng. *Internet Protocol*)
GDPR	Zakonska regulativa (eng. *General Data Protection Regulation)*
DPIA	Analiza utjecaja na zaštitu podataka (eng. *Data Protection Impact Assessment)*
DVR	Digitalni video snimač (eng. *Digital Video Recorder*)
VHS kazete	Zastarjele video kazete (eng. *Video Home System)*
VMS	Vrsta programske podrške (eng. *Video Management System)*
NAS	Mrežna pohrana podataka (eng. *Network Attached Storage*)
WDR	Široki dinamički raspon (eng. *Wide Dynamic Range*)
CODEC	Kompresija i dekompresija video podataka (eng. *Compression-Decompression*)
HDD	Tvrdi disk (eng. *Hard Disk Drive*)
CCD i CMOS	Tehnologije senzora slike (eng. *Charge-Coupled Device and Complementary Metal-Oxide-Semiconductor*)
VGA	Standard za prikaz slika (eng. *Video Graphics Array*)
Full HD	Vrsta razlučivosti slike (eng. *Full High Definition*)
AWB	Automatska ravnoteža bijele boje (eng. *Auto White Balance*)
LED	Vrsta diode (eng. *Light Emitting Diode*)
IR cut filter	Optički filter (eng. *Infrared Cut Filter*)
PTZ	Vrsta kamere (eng. *Pan-Tilt-Zoom*)
NVR	Mrežni snimač (eng. *Network Video Recorder*)
CPU	Centralna procesorska jedinica (eng. *Central Processing Unit*)
RAM	Radna memorija (eng. *Random Access Memory*)
HDMI	Digitalno sučelje za prijenos podataka (eng. High-Definition Multimedia Interface)
OS	Operativni sustav (eng. *Operating System*)
SSD	Vrsta pohrane podataka (eng. *Solid-State Drive*)
PoE	Napajanje preko Ethernet-a (eng. *Power over Ethernet*)
DCT	Diskretna kosinusna transformacija (eng. *Discrete Cosine Transform)*
MJPEG	Standard kompresije slike (eng. *Motion Joint Photographic Experts Group*)
AVC	Napredno video kodiranje (eng. *Advanced Video Coding*)

HEVC	Visoko učinkovito video kodiranje (eng. *High Efficiency Video Coding)*
SNMP	Protokol za upravljanje i nadzor mrežnih uređaja (eng. *Simple Network Management Protocol*)
RG11 i RG59	Oznake za vrste koaksijalnog kabela
BNC konektor	Tip konektora za prijenos analognog signala(eng. *Bayonet Neill–Concelman*)
AHD	Tehnologija za prijenos analognog signala (eng. *Analog High Definition*)
SFTP	Vrsta upletenenih parica (eng. *Shielded Foiled Twisted Pair*)
RJ-45 konektor	Oznaka za vrstu konektora upletenih parica (eng. *Registered Jack 45)*
T-568A i T-568B	Oznake za standarde ožičavanja upletenih parica i konektora
CAT	Oznaka za kategoriju kabela (eng. *Category*)
SC i LC	Oznake za optičke konektora (eng. *Subscriber Connector and Lucent Connector*)
SFP	Modularni optički priključak (eng. *Small Form-factor Pluggable*)
WLAN	Bežična lokalna mreža (eng. *Wireless Local Area Network*)
ASIC	Integralni sklop specifičan za primjenu (eng. *Application-Specific Integrated Circuit*)
PPM	Pikseli po metru (eng. *Pixels Per Meter*)
fps	Brzina okvira (eng. frames per second)
LPR/ANPR	Tehnologije za prepoznavanje registarskih oznaka (eng. Licence *Plate Recognition*/*Automatic Number Plate Recognition*)
OCR	Optičko prepoznavanje znakova (eng. *Optical Character Recognition*)
COCO	Skup podataka koji se koristi u računalnom vidu i strojnom učenju (eng. *Common Objects in Context*)
PP/J	Oznaka za fleksibilni PVC izolirani napajački kabel
Mpx	Megapikseli (eng. *Megapixels*)
FTPcat7	Oznaka za vrstu mrežnog kabela (eng. *Foiled Twisted Pair Category 7*)
VSDT	Programski paket (eng. *Video System Design Tool*)

SAŽETAK I KLJUČNE RIJEČI

Poglavlje o povijesti IP sustava videonadzora pruža uvid u evoluciju tehnologije od tradicionalnih analognih sustava prema modernim digitalnim sustavima temeljenim na IP protokolu. Osnovne komponente videonadzora detaljno su razrađene, uključujući IP kamere, mrežni snimač, mrežnu infrastrukturu te mrežni preklopnik. Osim toga, istražuje se i uloga videoanalitike koja omogućava automatizirano prepoznavanje uzoraka, detekciju događaja te analizu videozapisa kako bi sustavi postali učinkovitiji i proaktivniji. Poseban naglasak stavljen je na projektiranje sustava videonadzora, gdje se detaljno analizira proces planiranja, dizajniranja i implementacije. Projektiranje sustava videonadzora zahtijeva preciznu analizu potreba korisnika, odabir odgovarajućih komponenata, razmatranje sigurnosnih i zakonskih aspekata te optimizaciju infrastrukture za optimalne performanse.

Ključne riječi: Sustavi IP videonadzora, tehnička zaštita, mrežni snimač i mrežni preklopnik, upletene parice, bitrate, detekcija i prepoznavanje, projektiranje

ABSTRACT AND KEYWORDS

The chapter on the history of IP video surveillance systems provides insight into the evolution of technology from traditional analog systems to modern digital systems based on the IP protocol. The basic components of video surveillance are elaborated in detail, including IP cameras, network video recorders, network infrastructure, and network switches. Additionally, the role of video analytics is explored, enabling automated pattern recognition, event detection, and video analysis to make systems more efficient and proactive. Special emphasis is placed on the design of video surveillance systems, where the process of planning, designing, and implementation is analyzed in detail. Designing video surveillance systems requires a precise analysis of user needs, selection of appropriate components, consideration of security and legal aspects, and optimization of infrastructure for optimal performance.

Keywords: IP video surveillance systems, technical security, network video recorder and network switch, twisted pairs, bitrate, detection and recognition, design