Primjena vizualne kriptografije u zaštiti digitalnih sadržaja

Smajić, Alma

Sveučilište Jurja Dobrile u Puli

Fakultet informatike

Diplomski studij informatike

ALMA SMAJIĆ

PRIMJENA VIZUALNE KRIPTOGRAFIJE U ZAŠTITI DIGITALNIH SADRŽAJA

Diplomski rad

Pula, svibanj 2024.

Sveučilište Jurja Dobrile u Puli

Fakultet informatike

Diplomski studij informatike

ALMA SMAJIĆ

PRIMJENA VIZUALNE KRIPTOGRAFIJE U ZAŠTITI DIGITALNIH SADRŽAJA

Diplomski rad

JMBAG: 0303082451, redovita studentica

Studijski smjer: Informatika

Kolegij: Kriptografija

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informacijske i komunikacijske znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Mentor: doc. dr. sc. Siniša Miličić

Pula, svibanj 2024.

IZJAVA O KORIŠTENJU AUTORSKOG DJELA

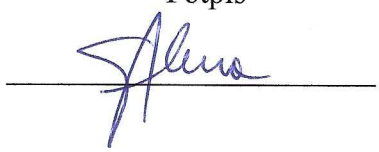
Ja, ALMA SMAJIĆ dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj diplomski rad pod nazivom PRIMJENA VIZUALNE KRIPTOGRAFIJE U ZAŠTITI DIGITALNIH SADRŽAJA

koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, 26. TRAVNJA 2024.

Potpis



IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani ALMA SMAJIĆ, kandidat za magistra INFORMATIKE ovime izjavljujem da je ovaj Diplomski rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Diplomskog rada nije napisan na nedozvoljeni način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

U Puli, 26. TRAVNJA 2024.

Sadržaj

1. Uvod

Suvremene informacijsko-komunikacijske i digitalne tehnologije omogućavaju nezamislivo brz protok informacija te sustavno i efektivno mijenjaju način obrade informacija, a posljedično time i njihove pohrane te u konačnici komunikacije.

U tom kontekstu, nastale promjene rezultiraju donošenjem brojnih pravila i zakona koji istovremeno pokušavaju dati slobodu izradi digitalnog sadržaja, a s druge strane i zaštititi same kreatore.

Govoreći o zaštiti, naglasak se stavlja na vizualnu kriptografiju – inovativnu, vizualnu metodu šifriranja i dešifriranja podataka koja koristi specifične tehnike podjele tajne informacije. Ova tehnika osigurava da tajnu nije moguće ni shvatiti, ni doznati iz pojedinačnih dijelova. Za razliku od dijeljenja tajni (eng. *secret sharing*), gdje se tajna informacija može rekonstruirati kombinacijom određenih dijelova, u vizualnoj kriptografiji nijedan samostalni dio nema informaciju o originalnoj slici što je dokazano i kroz tehničke primjere.

Rad se sastoji od četiri glavna poglavlja uz popratne tehničke primjere implementacije u Pythonu. Prvo poglavlje daje općeniti, kratak pregled što je kriptografija i koje sve vrste kriptografije postoje. Drugo poglavlje ulazi u srž i klasifikaciju same vizualne kriptografije te iznosi osnovna načela kako ista funkcionira, koje su vrste (sa pripadajućim primjerima u *Pythonu*), dok je treće poglavlje rezervirano za primjere i primjene u stvarnom životu (eng. *real life*) uz kratka pojašnjenja kako se točno odvija „proces u pozadini“. Četvrto, ujedno i posljednje poglavlje, fokusira se na predviđanje očekivanih trendova upotrebe.

U konačnici, tema sama po sebi otvara nova pitanja sigurnosti, financijske i tehničke mogućnosti i sposobnosti, ali nudi i potencijal za razvoj novih metoda šifriranja.

2. Općenito o kriptografiji

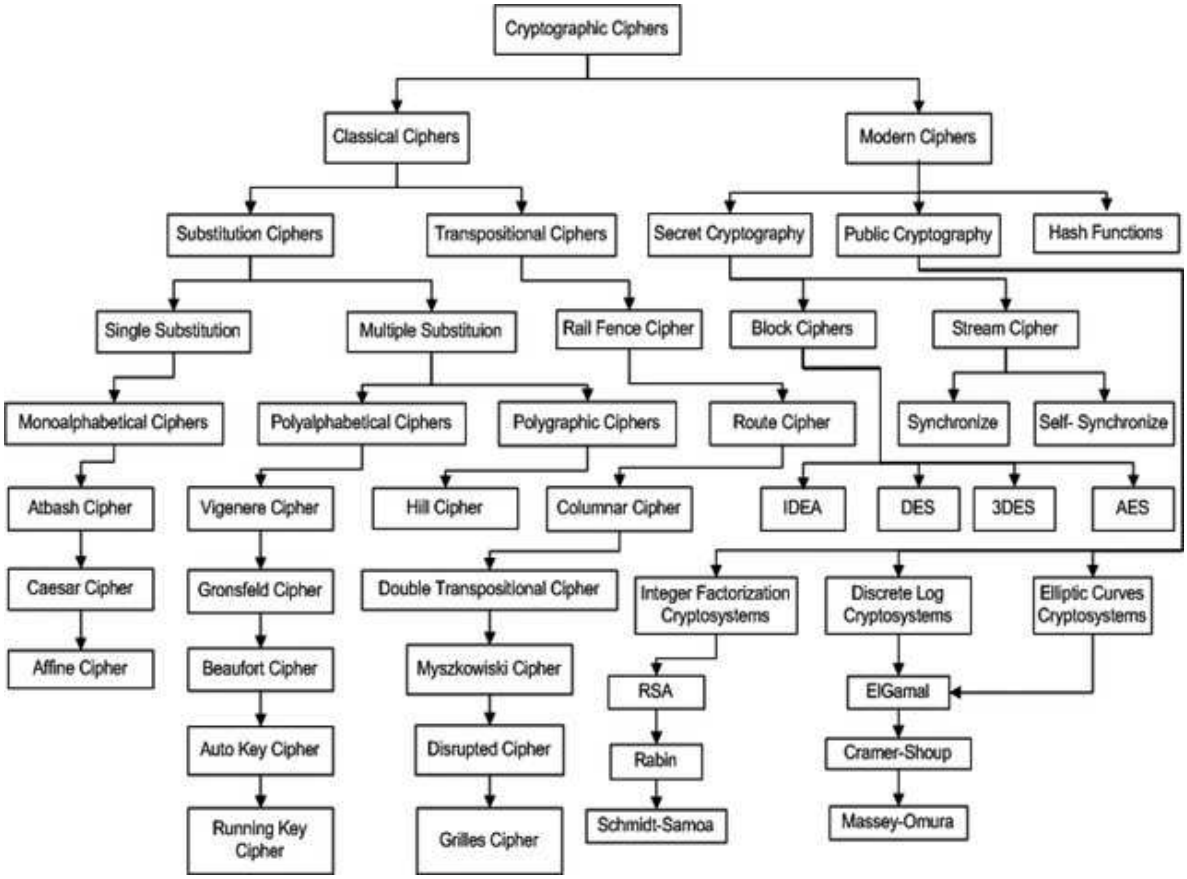
Za početak, prema Dujelli i Marcetiću, kriptografija je *znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati*. [1]

Kao takva, gledano na najširu sliku, kriptografija se dijeli na:

- simetričnu i asimetričnu kriptografiju, gdje:
    - **simetrična** – koristi jedan ključ (isti) i za enkripciju (šifriranje) i za dekripciju (dešifriranje). Ovdje se smjestila i vizualna kriptografija na kojoj počiva cjelokupni diplomski rad. Kao takva, umjesto matematičkih algoritama, za enkripciju podataka koristi vizualne fragmente slike. Dodatno, a i u usporedbi s ostalim vrstama kriptografije, tajne informacije prikazuje kroz više slika. Ovdje se još ubrajaju:
        - **kriptografija blokova** – šifriranje blok po blok koji je fiksne veličine, dok su otvoreni tekst (eng. *plaintext*) i šifrirani tekst (eng. *ciphertext*) zadani u bitovima, npr. AES[1] i DES[2]
        - **kriptografija toka** – enkripcija i dekripcija se odvijaju kontinuiranim tokom tako da se svaki bit kombinira sa pseudo-slučajnim bitom, npr. Salsa20 ili ChaCha[3]
    - **asimetrična** – koristi dva različita ključa; **javni** – ključ kojim se šifrira tajna poruka i **tajni** – ključ kojim se dekriptira, npr. RSA[4]

Detaljnijim razmatranjem klasifikacije glavnog pojma [2], podjela je zapravo puno kompleksnija kao što to prikazuje slika 1. Iako djeluje nezamislivo da postoji toliko kriptograma, uočena je manjkavost na ovom poprilično vizualno razgranatom prikazu. Radi se o nedostatku Diffie-Hellman protokola koji se smatra začetnikom kriptografije javnog ključa nakon kojeg su uslijedili slavni RSA i ECC.

[1] *Advanced Encryption Standard*
[2] *Data Encryption Standard*
[3] Salsa20 u svom generiranju pseudoslučajnih bitova koristi operacije rotacije i XOR-a, a obzirom na duljinu ključa (128 ili 256 bitova) koristi se u aplikacijama koje zahtijevaju brzu enkripciju. S druge strane, ChaCha je varijacija Salse20.
[4] Rivest-Shamir-Adleman



Slika 1. Kompleksnost klasifikacije kriptografskih algoritama: Jung, Ki-Hyun; Srinivasan, Ramakrishnan (Cryptographic and Information Security Approaches for Images and Videos, 2019.)

Većina šifrata može se zapisati matematičkim modelom koji se u kriptografiji naziva kriptosustav.

Kriptosustav je uređena petorka $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

1. $\mathcal{P}$ *je skup svih mogućih osnovnih elemenata otvorenog teksta*
2. $\mathcal{C}$ *je skup svih mogućih osnovnih elemenata šifrata*
3. $\mathcal{K}$ *je prostor ključeva, tj. skup svih mogućih ključeva*
4. *Za svaki* $K \in \mathcal{K}$ *postoji funkcija šifiranja* $e_K \in \mathcal{E}$ *i odgovarajuća funkcija dešifriranja* $d_K \in \mathcal{D}$. *Pritom su* $e_K : \mathcal{P} \to \mathcal{C}$ i $d_K : \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da je* $d_K(e_K(x)) = x$ *za svaki otvoreni tekst* $x \in \mathcal{P}$.

Definicijom kriptosustava potvrđujemo preslikavanje obje funkcije (enkripcija – šifriranje i dekripcija – dešifriranje) osnovnih elemenata otvorenog teksta (npr. slova, brojevi ili bitovi) koji se biraju iz određene familije. Kao posljednje, ostaje definirati prostor ključeva, opisan kao skup svih mogućih vrijednosti ključeva.

Za daljnje potrebe, kratki pregled izlistan na uvodnoj stranici bit će dostatan za kvalitetno i jednostavno praćenje ostatka rada.

3. Uvod u vizualnu kriptografiju

Godine 1994., kriptografi Moni Naor i Adi Shamir, uvode vizualnu kriptografiju i naglašavaju kako „*za novi tip kriptografske sheme, koji može dekriptirati skrivene slike, nisu potrebni složeni kriptografski izračuni*“ [3]. Predstavljena vrsta kriptografije naziva se vizualna kriptografija i usko je povezana s ljudskim vidnim sustavom.

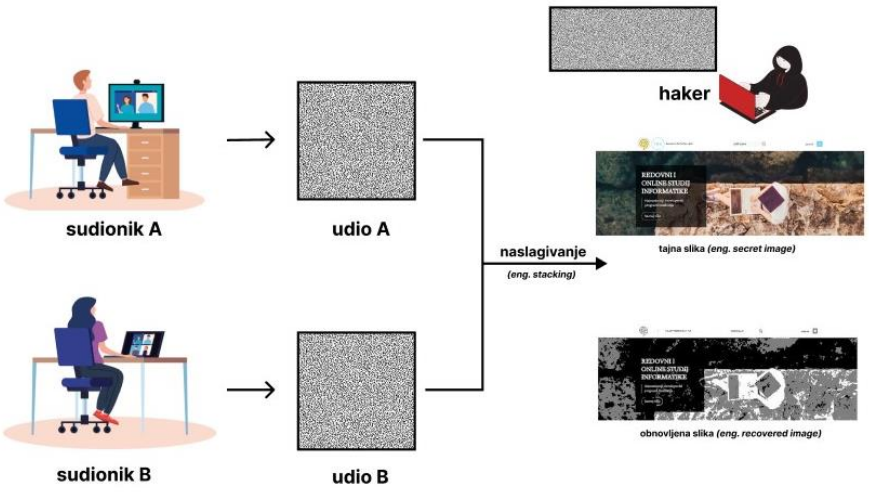
Za početak, potrebno je razumjeti da je dijeljenje slika podskup dijeljenja tajni, a tajne u ovom slučaju skrivene slike. Svaku tajnu, tj. sliku, tretiramo kao broj što omogućuje specifičnu shemu kodiranja za svaki izvor. Shema se definira kao *(k, n)* dijeljenje slika gdje:

- *k* – predstavlja broj dijelova koji su potrebni za potpuno uspješnu dekripciju
- *n* – predstavlja broj udjela (eng. *shares*)

Sigurna komunikacija funkcionira tako što se slika podijeli u više udjela koji se zatim naslaguju (eng. *stacking*). Na takav način jednom preklopljeni udjeli čine izvornu sliku. Pritom valja naglasiti da udio (sam za sebe) predstavlja samostalan, nedostatan dio za dobivanje početne informacije.

Slika 2 ilustrira inicijalnu implementaciju koja pretpostavlja da je slika kolekcija crnih i bijelih piksela. Svakim se pikselom upravlja individualno, dok bijeli piksel predstavlja prozirnu boju. Enkripcijski problem opisan je kao:

k od *n* problema dijeljenja tajni



Slika 2. Vizualni prikaz jednostavnog modela

U suštini, dana slika generira n prozirnosti tako da je originalna slika vidljiva ako se bilo kojih k prozirnosti naslaže zajedno, u protivnom ostaje skrivena. Iz toga slijedi da se struktura može zapisati kao $n \times m$ Booleova matrica S:

$$S = (s_{ij})_{m \times n} \quad \text{gdje je } s_{ij} = 1 \text{ ili } 0$$

Dok m predstavlja broj crno-bijelih piksela u udjelu, tj. gubitak rezolucije od originalne slike do obnovljene.

U konkretnom primjeru, matrica bi izgledala:

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \text{ iz čega slijedi da je } A \times B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Python kodom, množenje matrica možemo zapisati kao:

```python
def mnozenje_matrica(matrica1, matrica2):
    if len(matrica1[0]) != len(matrica2):
        raise ValueError("Matrice ovih dimenzija nije moguće množiti.")

    rezultat = []

    for i in range(len(matrica1)):
        red = []
        for j in range(len(matrica2[0])):
            red.append(False)
        rezultat.append(red)

    for i in range(len(matrica1)):
        for j in range(len(matrica2[0])):
            for k in range(len(matrica2)):
                rezultat[i][j] |= matrica1[i][k] and matrica2[k][j]

    return rezultat

booleova_m1 = [
    [1, 1, 0],
    [0, 1, 1],
```

```
    [1, 1, 0]
]

booleova_m2 = [
    [0, 0, 1],
    [0, 0, 1],
    [1, 1, 1]
]

rez_mnozenja = mnozenje_matrica(booleova_m1, booleova_m2)
print("\nRezultat množenja Booleovih matrica:")
for red in rez_mnozenja:
    print(red)
```

I pripadajući output:

```
Rezultat množenja Booleovih matrica:

[0, 0, 1]
[1, 1, 1]
[0, 0, 1]
```

Ukratko, u praktičnom primjeru, dva sudionika unutar jednostavnog modela međusobno dijele udjele (udio A i udio B) koji naslagivanjem daju konačnu, tajnu sliku. Haker, kao osoba izvan kriptosustava, obzirom da ne zna informacije o udjelima, nema pristup informaciji (slici) koja se prosljeđuje.

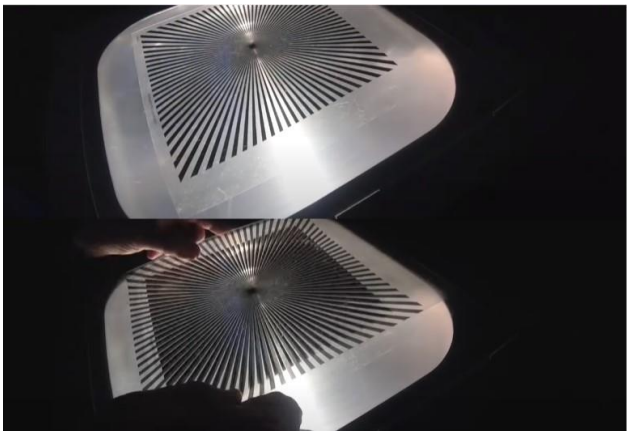
Jednostavni model[5] (eng. *basic model*), na slici 2, sastoji se od šifrata koji može biti poslan mailom i tajnog ključa (eng. *secret key*) koji će u nastavku biti definiran kao transparenti ili prozirnice/folije (eng. *transparencies*). Grafički su prikazani kao udio A i udio B.

[5] Jednostavni model izrađen je u Figmi i koristi grafike za koje nije potrebno licenciranje, dok je praktičan primjer vizualni prikaz teorijskih objašnjenja.

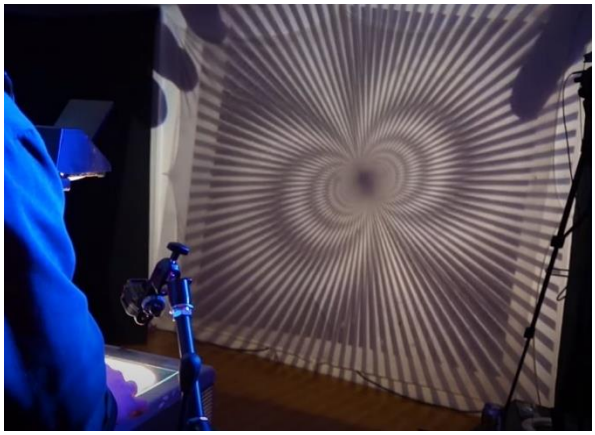
Originalni šifrat (logo fakulteta) otkriven je tek u trenutku postavljanja folija sa ključem na stranicu šifrata sa drugačijom folijom, odnosno naslagivanjem (eng. *stacking*).

Promatranjem dva nasumično točkasta uzorka (eng. *dot pattern*), čitač mora fotokopirati svaki uzorak na zasebnu prozirnost kako bi dekriptirao tajnu poruku (eng. *secret message*), oprezno ih poravnati i zatim osvijetliti rezultat grafoskopom. [4]

Slika 3 prikazuje jedan takav primjer i postavljanje jedne, a zatim i druge folije metodom naslagivanja, dok slika 4 prikazuje kako izgleda konačni motiv nakon preklapanja obje folije izložene svjetlu grafoskopa.

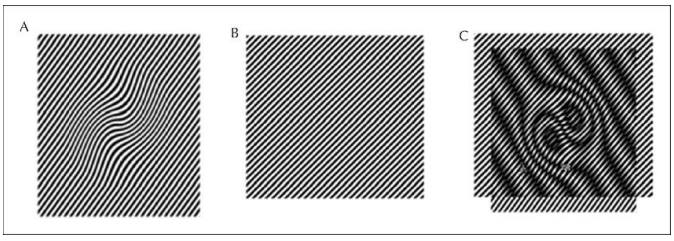


Slika 3. Postavljanje prozirnosti na grafoskop



Slika 4. Konačni motiv nastao naslagivanjem/preklapanjem

U ovom slučaju, umjetnik je nastojao prikazati motive crteža poznatog Moiréovog efekta, što slika 5 efektno dočarava kroz računalni prikaz. [5]

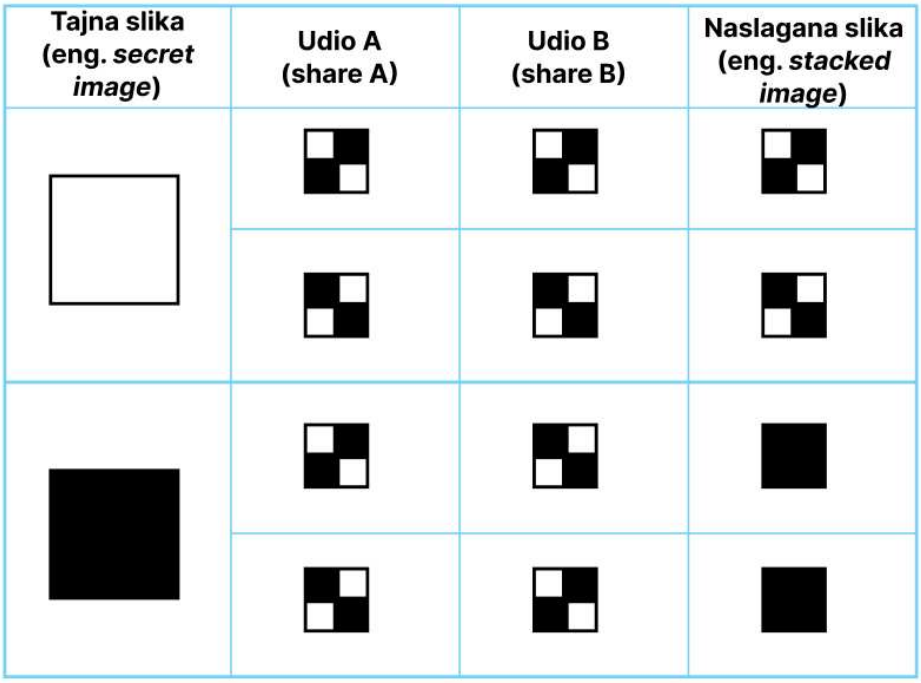


Slika 5. Računalni prikaz Moiréovog efekta

Računalni prikaz se zasniva na konstrukciji koja je u literaturi poznata kao (2,2) – VCS, gdje *m=2*, a VCS predstavlja kraticu za shemu vizualne kriptografije (eng. *visual cryptography scheme*).

Metoda proširenja piksela, vidljiva na slici 6, pokazuje kako su Naor i Shamir definirali dijeljenje udjela. Sve započinje sa tajnom slikom kojoj je početni piksel bijeli ili crni, što je statistički gledano vjerojatnost od 50%. Udjeli se generiraju kako slijedi:

- ukoliko je piksel originalne binarne slike bijeli, nasumično izaberite uzorak preostala 3 piksela (od ukupno 4) za oba udjela
- ukoliko je piksel originalne binarne slike crni, izaberite komplementaran par uzoraka (npr. iste stupce)



Slika 6. Naor i Shamirovo proširenje piksela

Ovo za sobom povlači i potencijalne nedostatke:

1. **ovisnost o ljudskom vizualnom sustavu –** prvenstveno uzimajući u obzir ranjivosti kao što su:
    a. problemi s kontrastom (određuje jasnoću oporavljene slike)
    b. ograničenja i percepcija ljudskog oka koja je individualna do povezanosti sa današnjim razvojem tehnologija
    c. razvoj računalnog vida koji je ponekad precizniji od ljudskog

2. **ograničenje slike**
    a. **povećana kompleksnost/složenost –** povećanjem broja „sudionika“ povećava se složenost upravljanja i distribucije prozirnosti što zahtijeva puno više resursa kod slika velikih razmjera (eng. *large scale image*)
    b. **kvaliteta** – postupak preklapanja može rezultirati lošijom kvalitetom u usporedbi sa originalom. To ujedno dovodi do gubitka detalja ili zamućenja što rezultira otežanom rekonstrukcijom slike visoke kvalitete.
3. **neovlaštena rekonstrukcija –** ukoliko neovlaštena osoba (na jednostavnom modelu, slika 2, prikazano kao haker) dobije pristup dovoljnom broj folija moguća je rekonstrukcija tajne slike bez pristanka ostalih sudionika
4. **jednostavnost** – koliko god ovo u početku zvučalo kao banalna prednost, toliko je i nedostatak, npr., ovakva metoda neprikladna je za slučajeve sa složenijim ili tekstualnim podacima

Kako su neki od ovih nedostataka bili iznimno očiti, istraživači su nastojali pronaći rješenja za njih. Neka od tih su:

1. **popravljena kvaliteta slika** – poboljšanje rezolucije i vjernosti tajne slike gdje se ističe ime Rakesh Agrawal
2. **robusnost protiv napada** – implementacija mjera u svrhu poboljšanja sigurnosti gdje se ističe Chiou-Ting Hsu
3. **„otežavanje“ jednostavnosti** – implementacijom vizualne kriptografije u složenije medije kao što su: dokumenti, videa pa čak i 3D modeli gdje se spominje ime Debasish Jena [6]

Za očekivati je da se i dalje radi na njima te njihovom napretku kako bi ostali kompliciraniji i ažurni sa aktualnim tehnologijama.

4. Klasifikacija vizualne kriptografije kroz tehničke primjere

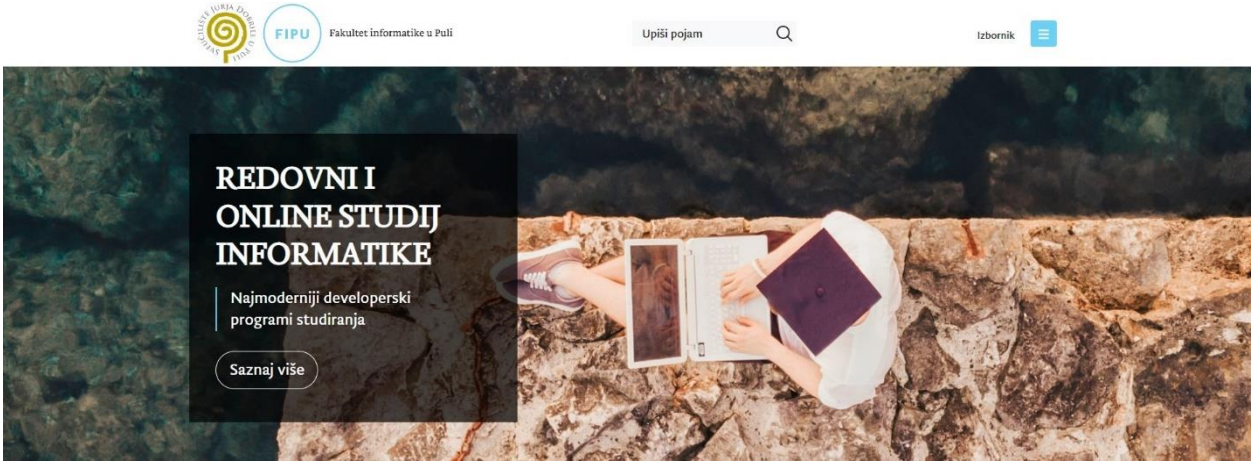
Za početak, potrebno je izabrati testnu sliku koja će nastojati pratiti svaku od izlistanih vrsta vizualne kriptografije. Najčešće se u području digitalnog procesiranja slika koristi *Lenna*, portret mlade žene na slici 7. Zbog izazovne i visoko-kontrastne pozadine (u usporedbi s licem), ona predstavlja simbol za evaluacijske eksperimente s algoritmima. Mnogi se na fotografiju referiraju kao „zlatni standard" jer ukazuje na važnost kvalitetnog testnog uzorka.

Slika 7. Lenna, najčešće korišteni model u digitalnom procesiranju

Postoji i druga strana priče zbog koje ju pojedinci izbjegavaju navoditi u svojim radovima ili istraživanjima. Spomenuta fotografija prvotno je objavljena 1972. u časopisu Playboy kada je djevojka sa fotografije imala samo 21 godinu. Uz titulu „Miss studenog", šest mjeseci kasnije, fotografija je došla i do „Instituta za obradu signala i slike" na Sveučilištu Južne Karoline gdje su ju Alexander Sawchuk i njegov tim iskoristili za testiranje najnovijeg algoritma kompresije. Iz društvenog aspekta, postoje i teorije kako bi se fotografija trebala umiroviti zbog raznih feminističkih, seksualnih i erotskih komentara koje vuče za sobom. Jedna takva, proizlazi iz 2013. godine kada su dvije profesorice na UCLA-i kupile prava na fotografiju modela koju su iskoristile u svom slikovnom istraživanju.

Neovisno o svemu što je pratilo Lenu, u svom životu je imala još jednu veliku suradnju; sa Kodakom. Njeno lice preplavilo je naslovnice stoga ni ne čudi činjenica da je ponosna na svoja životna djela. Jedino za čime donekle žali jest što nije potraživala veću naknadu od prisvajanja slike i titule „zaštitnice JPEG-a". [7]

Neovisno što nije nužno povezana sa erotskim i akademski neprimjerenim sadržajem, izostavljena je pri dubljoj analizi i obradi slika kroz rad. U svrhu pokazivanja tehničkih primjera kroz četiri vrste vizualne kriptografije, koristila sam programski jezik *Python*, radno okruženje *Jupyter Notebook*-a na lokalnom serveru `localhost:8888` te naslovnu (vodeću) sliku koja je trenutno dostupna na mrežnim stranicama Fakulteta informatike u Puli [8], a vidljiva je na slici 8.

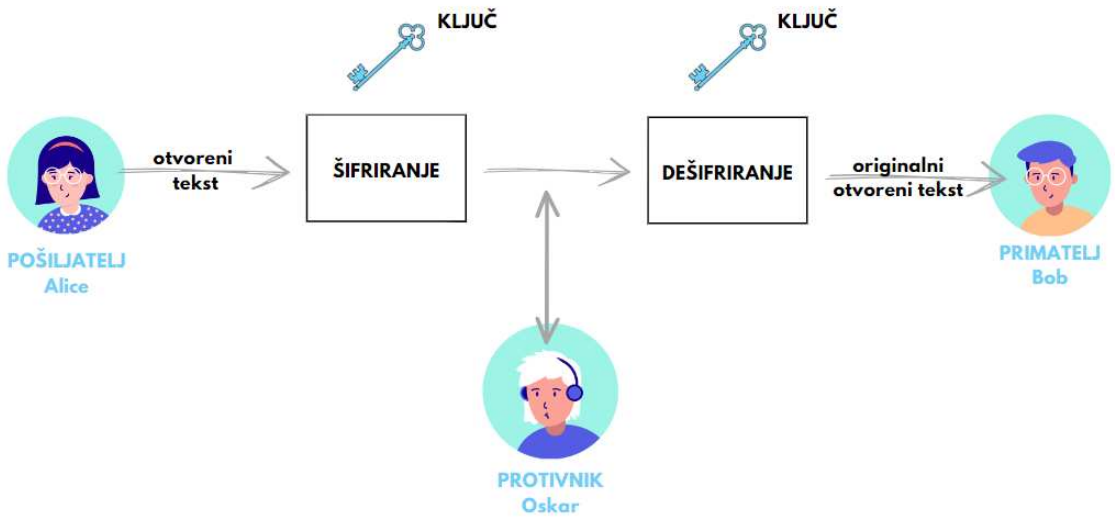


Slika 8. Vodeća slika naslovnice FIPU-a, studeni 2023.

Nepromijenjena slika kao takva, zapravo je kontinuiranog tona što je u suštini, gdje jedna boja završi – druga započne. Pikseli koji nose tajne informacije predefinirani su ljudskom oku nevidljivom promjenom/manipulacijom kako bi sadržali sve tajne informacije prije transformacije u nijanse sivih tonova. Time bi se umanjila mogućnost distorzije, tj. promjene izgleda slike koja se najčešće odnosi na izobličenje ili promjenu perspektive.

Ostaje nam još definirati osnovni zadatak kriptografije. Modelom na slici 9 pokazujemo poopćeni model gdje je komunikacija omogućena između 2 osobe (pošiljatelj i primatelj), u literaturi poznati kao Alice i Bob, kroz nesiguran komunikacijski kanal (npr. računalna mreža) na takav način da treća osoba (njihov protivnik, npr. Eva ili Oskar) može nadzirati komunikacijski kanal, ali ne može razumjeti njihove poruke.

Poruku koju pošiljatelj, npr. Alice, želi poslati primatelju, Bobu, naziva se otvoreni tekst (eng. *plaintext*). Pošiljatelj transformira otvoreni tekst koristeći unaprijed dogovoreni ključ. Taj postupak nazivamo šifriranje (enkripcija), dok se dobiveni rezultat naziva šifrat (eng. *ciphertext*). Nakon toga, pošiljatelj pošalje šifrat preko komunikacijskog kanala, a primatelj koji zna ključ kojim je šifrirana poruka može dešifrirati (dekriptirati) šifrat i odrediti otvoreni tekst. U našem slučaju, kroz kontekst vizualne kriptografije, jasno je da Alice i Bob umjesto teksta razmjenjuju slike, odnosno udjele, a sve ovisno o promatranoj vrsti.



Slika 9. Kriptografski model komunikacije (autorski rad po uzoru na Dujellu)

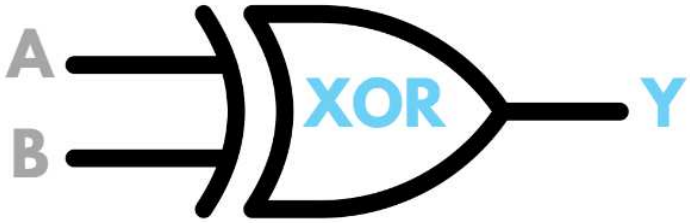
Spomenute vrste na kojima će se provoditi enkripcija i dekripcija, složene prema težini, su:

- vizualna kriptografija bazirana na XOR-u – šifriranje tajne slike u *n* značajnih udjela koji mogu uvesti *n* naslovnih slika. Operacijom XOR moguće je vratiti izvornu sliku. [9]
- vizualna kriptografija iz difuzije polutonskih pogrešaka – pogreške kvantizacije se raspršuju na „buduće“ piksele, tj. ostatak kvantizacije distribuiran je na susjedne piksele koji još nisu obrađeni [10]
- vizualna kriptografija za više tajni
- proširena vizualna kriptografija za slike u boji – svaki piksel tajne slike u boji proširuje se u blok veličine 2x2 kako bi se formirale dvije zajedničke slike. Svaki 2x2 blok na dijeljenoj slici ispunjen je crvenom, zelenom, plavom i bijelom (prozirnom)

redom pa se nijedan trag o tajnoj slici ne može identificirati samo iz (bilo koja) dva dijeljenja [11]

4.1. Vizualna kriptografija bazirana na XOR-u

XOR ili isključivi OR (eng. *exclusive OR*) logička je operacija koja se primjenjuje na dva ulaza, u ovom slučaju piksela, i daje izlaz koji je istinit (1) samo kada su ulazi različiti, tj. ne mijenja stanje kada se primjenjuje na iste binarne vrijednosti što prikazuje slika 10.



A	B	Y
0	0	0
0	1	1
1	0	1
1	1	1

Slika 10. Isključivi OR, autorska kreacija bazirana na predznanju

Slika 11 prikazuje isti primjer sa pikselima gdje možemo reći da vrijednost 0 predstavlja odsutnost boje (crna), a vrijednost 1 predstavlja prisutnost boje (bijela).

Ulazni pikseli (eng.*entry pixel)*	XOR-an rezultat (eng. *XOR result)*
■ ■	■
■ □	□
□ ■	□
□ □	■

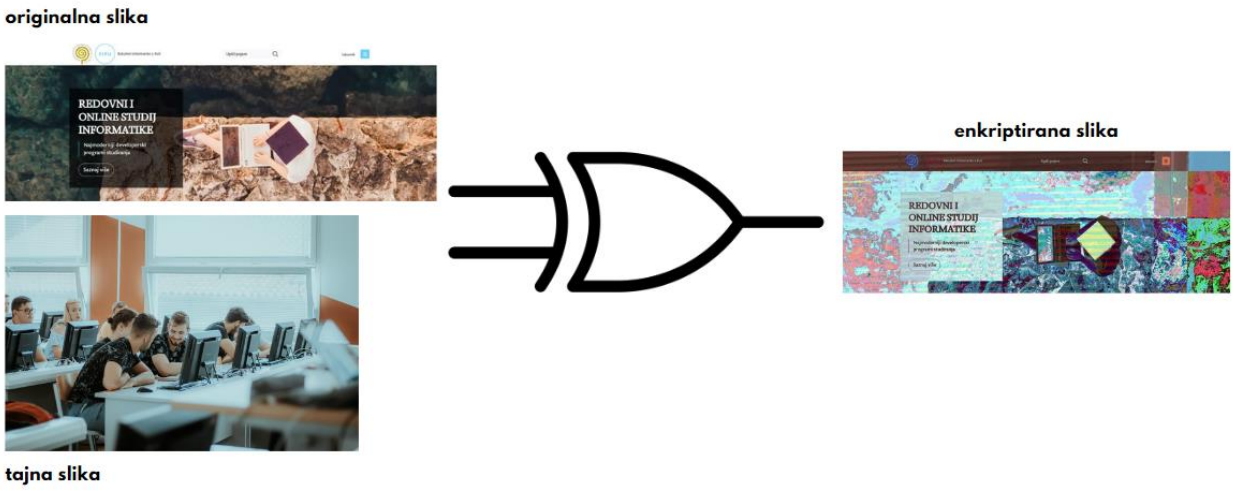
Slika 11. XOR u kontekstu piksela

XOR bazirana kriptografija rješava problem loše vizualne kvalitete u tradicionalnim shemama vizualne kriptografije [12]. Razvijena je za postizanje boljeg kontrasta i rezolucije rekonstruirane slike što prikazuje kod niže.

```
from PIL import Image

# Definiranje XOR funkcije;
def xor_encrypt_decrypt(image1, image2):
    encrypted_image = Image.new("RGB", image1.size)
    decrypted_image = Image.new("RGB", image1.size)

    width, height = image1.size

    # Iteracija kroz piksele po koordinatama
    for x in range(width):
        for y in range(height):
            # Dohvacanje koordinata piksela
            pixel1 = image1.getpixel((x, y))
            pixel2 = image2.getpixel((x, y))

            # XOR nad RGB vrijednostima piksela
            encrypted_pixel = tuple(p1 ^ p2 for p1, p2 in zip(pixel1, pixel2))
             decrypted_pixel = tuple(p1 ^ p2 for p1, p2 in zip(encrypted_pixel,
pixel2))

            # Postavljanje piksela u enkriptiranu i dekriptiranu sliku
            encrypted_image.putpixel((x, y), encrypted_pixel)
            decrypted_image.putpixel((x, y), decrypted_pixel)

    return encrypted_image, decrypted_image

leading_image_path  =  r'C:\Users\almas\Desktop\Diplomski\Diplomski-rad\vodeca-
slika.jpg'
second_image_path        =        r'C:\Users\almas\Desktop\Diplomski\Diplomski-
rad\novosti_vodeca.jpg'

# Ucitavanje slika
```

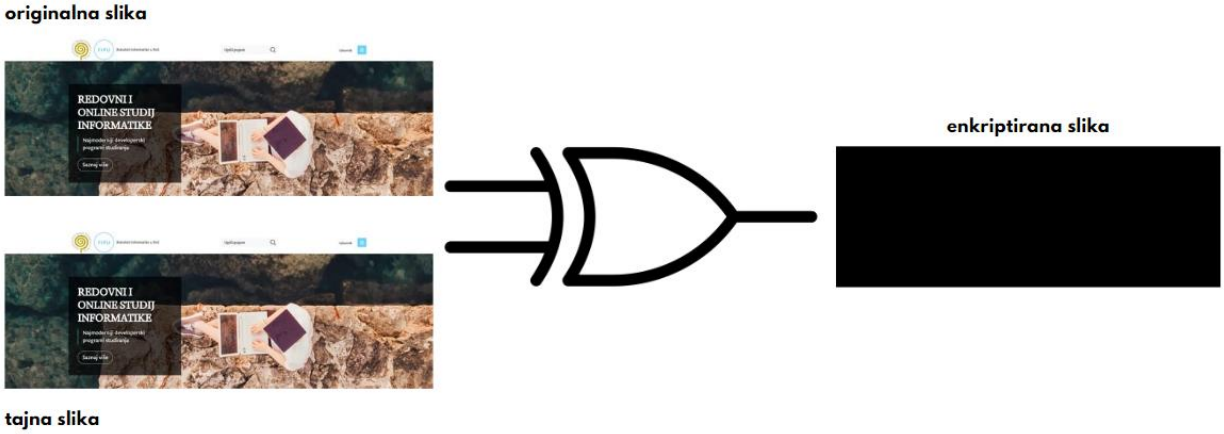
```
leading_image = load_image(leading_image_path)
second_image = load_image(second_image_path)

if leading_image and second_image:
    # Enkripcija i dekripcija
        encrypted_img,   decrypted_img   =   xor_encrypt_decrypt(leading_image,
second_image)

    # Pohrana enkriptirane i dekriptirane slike
    encrypted_img.save("enkriptirana_fipu-xor.jpg")
    decrypted_img.save("dekriptirana_fipu-xor.jpg")
```

Na slici 12 vidljiva je originalna slika, vodeća slika mrežne stranice FIPU-a, nad čijim smo RGB vrijednostima proveli XOR operaciju, a zatim smo uveli **novu**, tajnu sliku (vodeća slika *Novosti* na FIPU mrežnoj stranici).



Slika 12. Vizualna kriptografija bazirana na XOR-u; uspješno skrivanje

Kroz cijeli proces, naglasak je na važnosti nove tajne slike kako bismo izbjegli potpuna preklapanja piksela. Slika 13 prikazuje XOR vizualnu kriptografiju gdje su vodeća i tajna slika iste, što je XOR operacijom rezultiralo vrijednostima nula, odnosno prikazalo sliku kao u potpunosti crnu. Jedina preinaka u kodu bila bi uklanjanje putanje za *second_image*.



Slika 13. Vizualna kriptografija bazirana na XOR-u; neuspješno skrivanje

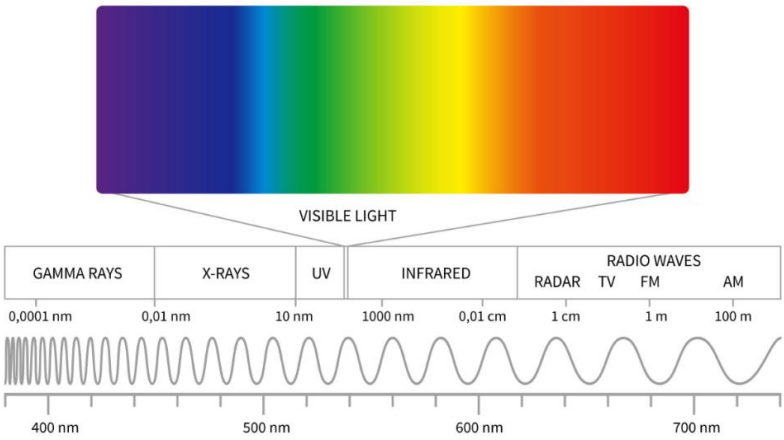
Enkripcija u ovom procesu ima za cilj šifrirati tajne slike mapiranjem zajedničkih slika koje nemaju problema s proširenjem piksela i ne otkrivaju nikakve informacije o tajnim slikama. Valja uzeti u obzir da se algoritam odabira nasumičnog stupca temelji na 0-mapiranju ili 1-mapiranju matrice gdje se dvije matrice dinamički generiraju u shemi šifriranja. Dekripcija iziskuje računalnu pomoć [13], ali ujedno pruža novi način optimizacije proširenja piksela i izobličenja kontrasta. Rekonstruirana slika tako ne trpi nikakvo izobličenje u usporedbi s izvornim tajnim slikama.

Ova vrsta vizualne kriptografije predstavlja napredak zbog svoje jednostavne strukture pristupa i multifunkcionalnosti neovisno o vrsti i boji slike. Trenutno najbolji dostupan primjer datira iz 2022. godine. Chen i Juan [14] su predstavili XOR-baziranu shemu za nijansirane ili tajne slike u boji. Shema enkriptira tajnu sliku u značajne udjele koji se mogu naslagivati koristeći XOR shemu kako bi se potpuno obnovila originalna tajna slika.

U stvarnim situacijama, kao i na našem primjeru, slike nikad neće biti predstavljene samo kao polutonske, odnosno kao binarne gdje se vidni sustav oslanja na „obični“ ILI (eng. *OR*) ili po sivoj skali.

Vizualna kriptografija za slike u boji je kompleksnija, ali neovisno o tome, interes za ovu vrstu postaje veći no ikad. [15] Za bolje shvaćanje boja potrebno je razumjeti pojmove poput:

- principa superpozicije – output mu je zbroj 2 ili više podražaja (u ovom slučaju boje) kako bi se dobila ukupna kombinacija. Primjerice, superpozicija valova crvene boje i plave boje jest ljubičasta boja.
- svjetla – odnosno vidljivo svjetlo dio je elektromagnetskog spektra između 380 *nm* - gdje se nalazi ljubičasta i 700 *nm* - gdje se nalazi crvena boja [16], što je vidljivo i na slici 14. Ove brojke proizlaze iz percepcije boja u trenutku kad određene valne duljine pogode mrežnicu ljudskog oka. [17] Primjenjuju se na većinu populacije i ako se iz primjera izuzmu moguće anomalije poput daltonizma, mono[6] i dikromatskog[7] vida, tritanopije[8], tritanomalije[9] i drugih



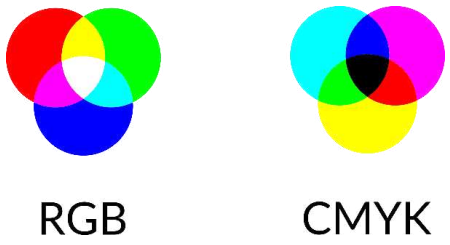
Slika 14. Spektar vidljive svjetlosti

- teorije boja – za neke znanost, za druge umjetnost korištenja boja, a u suštini objašnjenje kako ljudi percipiraju boje te kako se iste međusobno miješaju, slažu i razlikuju jedna od druge

[6] Monokromatski vid – percepcija svijeta u crno-bijeloj skali
[7] Dikromatski vid – ograničena sposobnost neraspoznavanja boja
[8] Tritanopija – nemogućnost razlikovanja plave i žute
[9] Tritanomalija – smanjena osjetljivost na plavu boju

Uzimajući u obzir skup svih mogućih boja svediv je na tri osnovne (primarne): crvena, žuta i plava boja [18] iako se zbog jednostavnosti koriste sljedeći komplementarni rasponi kao što prikazuje slika 15:

- RGB – *red, green, blue*
- CMY i CMYK [19]– *cyan, magenta, yellow* i *black*



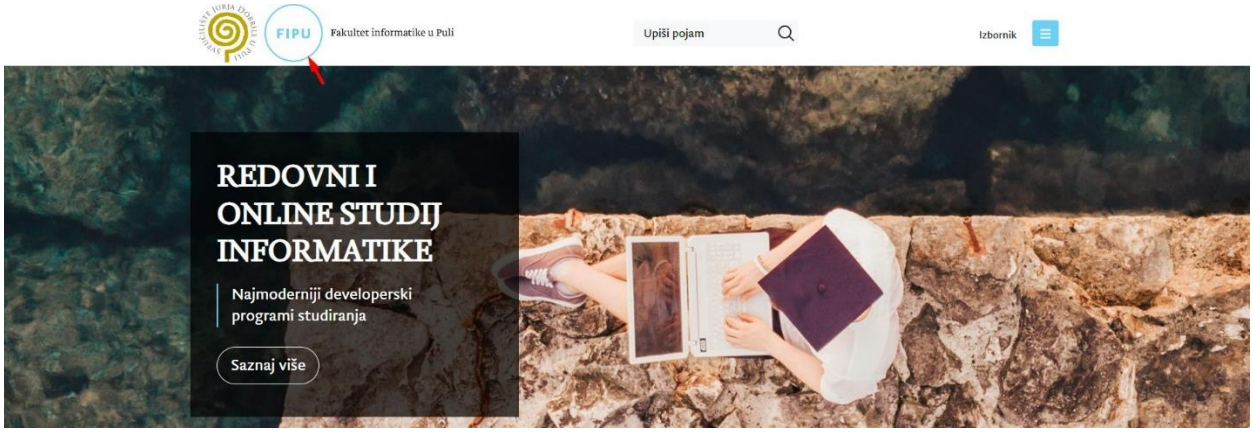
Slika 15.RGB i CMYK prikazi boja

Niže priloženi kod opisuje kako prethodno objašnjena XOR operacija prolazi kroz svaki od RGB kanala i provodi enkripciju, a zatim i dekripciju vodeće slike.

```
from PIL import Image

def encrypt_decrypt_image(image_path, key):
    original_image = Image.open(image_path)

    # Pretvorba slike u niz piksela
    pixels = original_image.load()
    width, height = original_image.size

    # Enkripcija
    encrypted_image = Image.new('RGB', (width, height))
    encrypted_pixels = encrypted_image.load()
    for i in range(width):
        for j in range(height):
            r, g, b = pixels[i, j]
            # XOR operacija kroz svaki kanal slike
            r = r ^ key
            g = g ^ key
            b = b ^ key
            encrypted_pixels[i, j] = (r, g, b)
    encrypted_image.show()

    # Dekripcija
    decrypted_image = Image.new('RGB', (width, height))
    decrypted_pixels = decrypted_image.load()
```

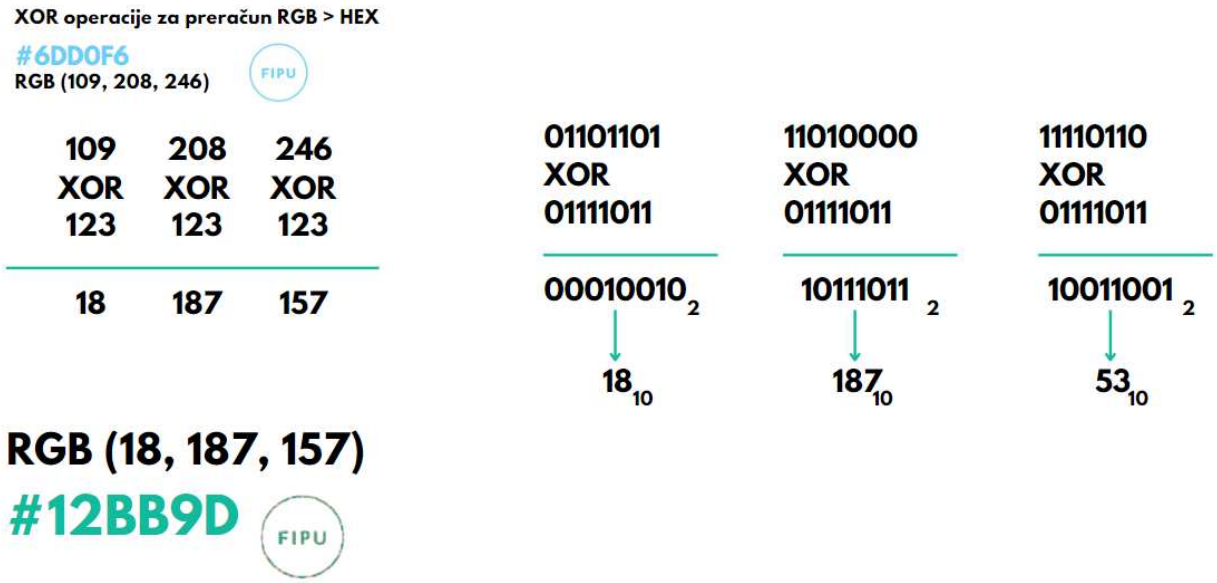
```
    for i in range(width):
        for j in range(height):
            r, g, b = encrypted_pixels[i, j]
            # XOR operacija kroz svaki kanal slike
            r = r ^ key
            g = g ^ key
            b = b ^ key
            decrypted_pixels[i, j] = (r, g, b)
    decrypted_image.show()

image_path = r'C:\Users\almas\Desktop\Diplomski\Diplomski-rad\vodeca-slika.jpg'

# Kljuc za enkripciju i dekripciju
key = 123

encrypt_decrypt_image(image_path, key)
```

Svaka od RGB vrijednosti može se prikazati kao trojka (x, y, z) gdje spomenuta slova predstavljaju količinu pojedine boje. Tri elementa moguće je gledati kao „filter“ koji propušta samo dio svjetla. Ilustrativni primjer bila bi boja (0, 0, 0) koja se prikazuje kao crna – svi filteri su crni što znači da nema svjetla. Općenito gledano, što je viša vrijednost komponente, boja je svjetlija. Za ilustrativni primjer, vidljiv na slici 16, iskoristit ćemo plavu boju vidljivu u logu čiji je HEX kod #6DD0F6, odnosno po RGB-u vrijednosti su (109, 208, 246).



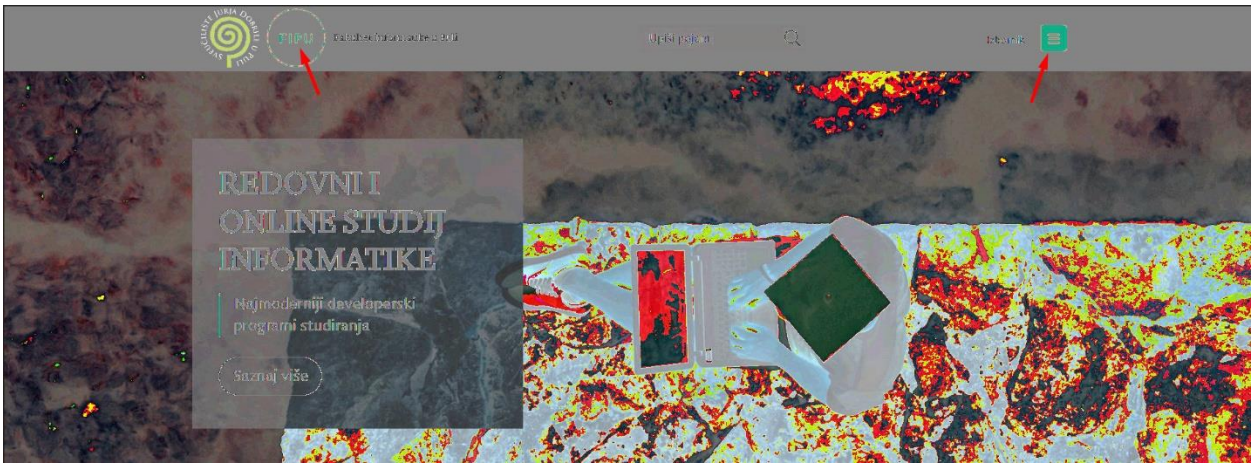
Slika 16. Prikaz originalne prije enkripcije (plava boja, #6DD0F6)

Nad njima ćemo provesti XOR sa ključem spomenutim u kodu koji iznosi 123 (proizvoljno zadan, uz minimalna ograničenja spomenuta kroz nadolazeći tekst) što prikazuje slika 17.



Slika 17. XOR operacija, a zatim preračun u HEX vrijednost

Dobivene vrijednosti (18, 187, 157) po RGB vrijednostima ćemo pretvoriti natrag u heksadecimalni zapis što rezultira sa #12BB9D i zelenkastim tonovima kao što je vidljivo na enkriptiranoj slici, tj. slici 18.



Slika 18. Uspješno enkriptirana slika (promjena u zelenu boju, #12BB9D)

Važno ograničenje, tj. napomena kod izbora ključa je da, ukoliko radimo sa XOR operacijom, ključ ne smije biti potencija broja 2 jer će rezultat biti kao da nema ključa. Svaki bajt originalne slike premješta se za 8 bitova u jednom smjeru pa drugom pri čemu uopće ne mijenja vrijednost. Razlog tomu je što se slika neće prikazati, tj. rezultira nedostatkom koji je poznat kao problem zatamnjivanja (eng. *darkening problem*). Opisan kao superponiranje piksela istih boja, uz iznimku nultih ili komponenti punog intenziteta, koji će rezultirati pikselom tamnije verzije od originalne boje. Do istog dolazi jer je svaka prozirnost filter koji apsorbira dio svjetla, osim kad je prozirnost bijela, gdje se „oduzima" svjetlo postavljajući filtere. Preostalo svjetlo određuje boju koja je vidljiva nakon superponiranja preostalih folija. Pretpostavka je da se započinje sa čistim bijelim svjetlom, odnosno da prozirnost nema tinte na sebi što omogućava jednostavan prodor svjetlosti vidljiv kao bijela boja. Iz toga slijedi jednostavan zaključak da je kapanjem određene tinte vidljiva boja koju propušta.

Ako se više folija naslaže (eng. *stacked*) jedna na drugu, boja piksela rezultata ovisi o svojstvima apsorpcije (upijanja) tinte na svim folijama.

Dodatno, važno je razlučiti i ova dva pojma:

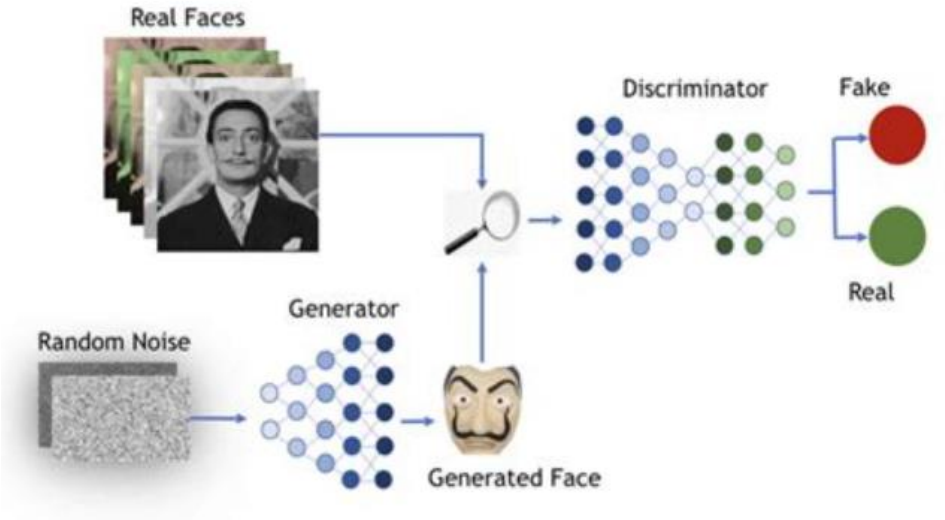
- **tajna paleta/paleta tajni** (eng. *secret palette*) – konačni skup boja koje se koriste u tajnoj slici
- **paleta udjela** (eng. *shares palette*) – skup boja koje je moguće printati na udjelima ili dobiti superpozicioniranjem ispisanih udjela. Ova paleta može biti jednaka originalnoj, ali moguće ju je i augumentirati sa jednom ili više drugih boja.

Kao što je već najavljeno, ova vrsta vizualne kriptografije je kompleksnija dobrim dijelom zbog nedovoljne istraženosti samog područja.

Dva su razloga:

1. **referentni model** – ne postoji definicija takvog iako bi najbolji primjer dočarao stvarni svijet. Svim slikama i modelom prikazanim kroz literaturu nedostaje dobro definiran kontrast što je vrlo važna mjera evaluacije.
2. **superpozicija boja** – konstrukcija je znatno teža u usporedbi sa crno-bijelim slikama

Neovisno o svemu i dalje se stremi jačim i boljim algoritmima te metodama šifriranja koje već sad pokazuju znakove otpornosti na neke napade, npr. GAN[10] vidljiv na slici 19. [20]

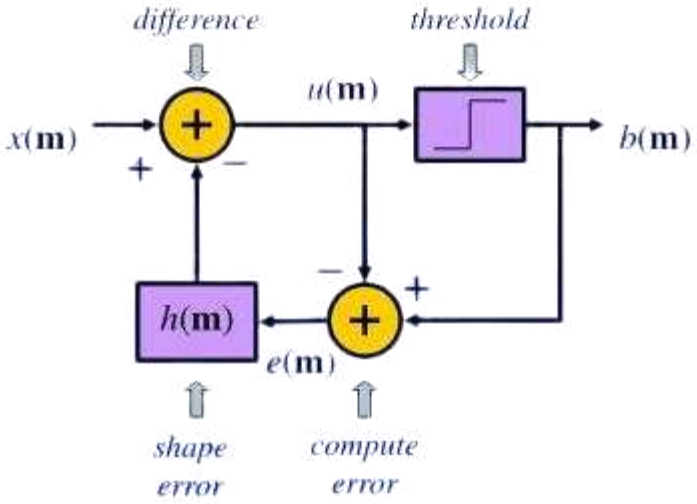


Slika 19. Princip rada GAN modela (MaungMaung, AprilPyone; Kiya, Hitoshi: StyleGAN Encoder-Based Attack for Block Scrambled Face Images, Itaca (Cornell University)

[10] *Generative Adversarial Network*, odnosno model dubokog strojnog učenja koji se sastoji od generatora (stvara lažne slike nalik originalnim) i diskriminatora (razlikuje originalne slike od generiranih lažnih)

4.2. Vizualna kriptografija iz difuzije polutonskih pogrešaka

Vizualna kriptografija bazirana na difuziji iz polutonske pogreške koristi tehnike polutoniranja (eng. *halftoning*) koju definiramo kao tehniku digitalne obrade slike pri čemu se kontinuirana siva slika pretvara u binarni uzorak crno-bijelih piksela. Tehnika se odvija u nelinearnom povratnom sustavu što se odnosi na procese: kvantizacije svakog piksela, filtriranje kvantizacijske greške (šuma) i dodavanja filtriranog izraza „budućim“ sivim pikselima radi razlaganja kvantizacijske greške kao što prikazuje Floyd-Steinbergov model na slici 20. [21]



Slika 20. Floyd-Steinbergov model difuzije polutonskih pogrešaka

Razvijeni model prikazuje proces kvantizacije ulaznog piksela, nakon čega se rezultirajuća kvantizacijska pogreška difuzira na susjedne piksele koji će uskoro biti procesirani. Izlazna vrijednost piksela ovisi o ulaznom pikselu i difuziranoj vrijednosti pogreške prethodnog piksela. Vrijednosti *x(m)* i *b(m)* su kontinuirane odnosno polutonirane slike gdje se ulazni piksel, tj. *x(m)* zbraja s vrijednosti prethodne pogreške piksela *p* i uspoređuje s pragom. Izlazni piksel, tj. *b(m)*, dobiva se iz usporedbe, dok se vrijednost *e(m)* računa oduzimanjem trenutne izlazne vrijednosti *b(m)* kombiniranom vrijednosti *h(m)* i *x(m)*. Posljednje, pogrešku *e(m)* množimo težinskim filterom prije difuzije na susjedne piksele. [22]

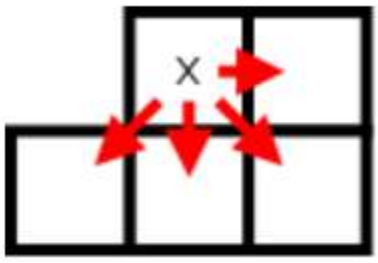
Uz taj model, veže se i Floyd-Steinberg polutoniranje koje smanjuje paletu boja slike (npr. kako bi se smanjila veličina datoteke slike) uz zadržavanje što više uočenih detalja. Glavna ideja očuvanja neke preciznosti boja jest osiguranje da „u prosjeku“ imamo pravi intenzitet svake komponente boje. To znači da ako trebamo uzeti dano područje polutonirane slike, prosjek crvene komponente svakog piksela treba biti, što je moguće, bliži prosjeku izvorne slike. [23] Spomenuto se postiže „guranjem“ greške (razlika u vrijednosti piksela, izvorno-novo) napravljene na jednom pikselu na njegove susjede, tako da kada su i oni kvantizirani, vjerojatnije je da će ispravno pridonijeti lokalnom prosjeku.

Matematička perspektiva to pokazuje kao: ako je x izvorna vrijednost piksela[11] i $\bar{x}$ njegov odabrani prikaz (npr. najbliža ponovljiva boja) tada je pogreška:

$$e = x - \bar{x}$$

Ako je vrijednost piksela koji trebamo pretvoriti u bijeli ili crni piksel bliža nuli, piksel se pretvara u crni. U protivnom – u bijeli. Problem nastaje u „hrpi 96 sivih“ piksela kada se svi pretvaraju u crne, a mi ostajemo s ogromnim dijelom praznih crnih piksela koji dobro ne predstavljaju izvornu sivu boju. Difuzija ovdje ima ulogu bilježenja „pogrešaka“ koje se šire u susjedstvu piksela. Konkretnim brojevima, pomak se vidi u kretnji na idući piksel kojem se dodaje pogreška od 96 što rezultira vrijednošću od 192, a samim time i bliže bijelom. Novi piksel se sada bilježi kao bijeli uz grešku koja iznosi -63 (192-255). Napredovanjem algoritma, difuzna pogreška rezultira naizmjeničnim točkastim (eng. *dot pattern*) uzorkom crnih i bijelih piksela. [24]

Difuziju kontrolira matrica difuzije prikazana na slici 21:



Slika 21. Difuzija Floyd-Steinbergove matrice

[11] Zanemarena je mogućnost da piksel može imati više od jedne komponente boje

Na kraju svake strelice nalazi se koeficijent koji određuje dio pogreške koji se šalje tom pikselu, a primjer na kojem se bazira i implementacija u kodu tiče se Floyd-Steinbergove matrice s djeliteljem 16. [25]

Broj 16 nije nasumično izabran već je proizašao dijeljenjem broja 96, predstavlja piksel tamnosive vrijednosti, na 6. Za svaki piksel u izvornoj slici, boja najbliža tom pikselu se odabire iz ograničene palete, dok se piksel u razmatranju označava * kao na slici 22:

$$\begin{matrix} 0 & 0 & 0 \\ 0 & * & \frac{7}{16} \\ \frac{3}{16} & \frac{5}{16} & \frac{1}{16} \end{matrix}$$

Slika 22. Floyd-Steingbergova matrica

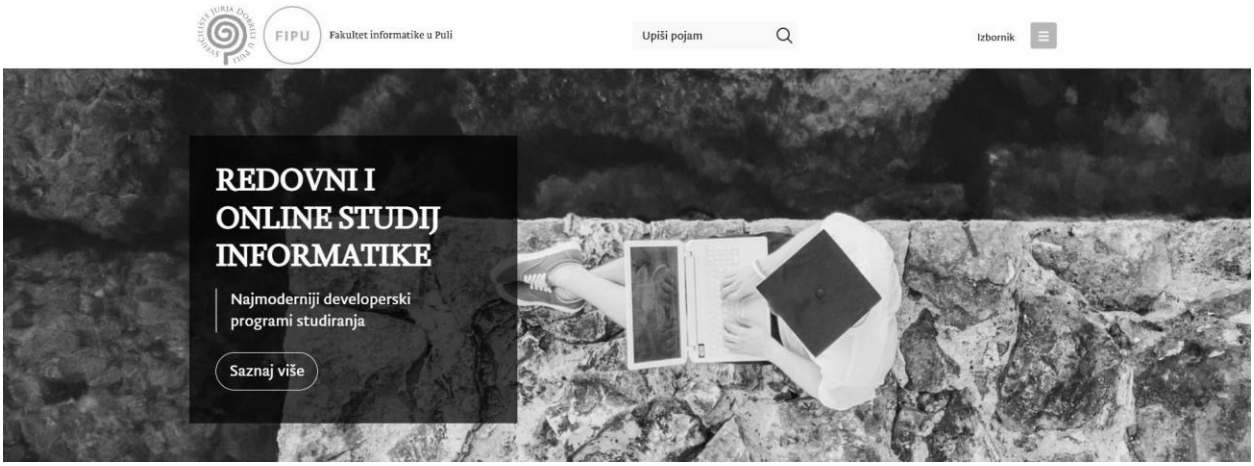
Budući da to ne utječe na piksele iznad i lijevo od piksela razmatranja, algoritam se primjenjuje na skeniranje slike jednom, odozgo prema dolje, tj. slijeva nadesno.

U nastavku slijedi tehnički primjer koda koji zaprima lokalno pohranjenu sliku koju smo prethodno koristili; vodeća slika s mrežne stranice FIPU-a.

Za početak, niže priloženim kodom smo pretvorili vodeću sliku iz „obične“ u sliku po sivoj skali, vidljivu na slici 23:

```
from PIL import Image

def img_to_gray_scale(img_path, save_path):
    original_img = Image.open(img_path)
    grayscale_img = original_img.convert("L")
    grayscale_img.save(save_path)

original_img_path   =   r'C:\Users\almas\Desktop\Diplomski\Diplomski-rad\vodeca-slika.jpg'
grayscale_img_path   =   r'C:\Users\almas\Desktop\Diplomski\Diplomski-rad\vodeca-slika_grayscale.jpg'

img_to_gray_scale(original_img_path, grayscale_img_path)
```

Preostali kod s popratnim komentarima, uz sliku 24, prikazuje procese šifriranja i dešifriranja gdje je:



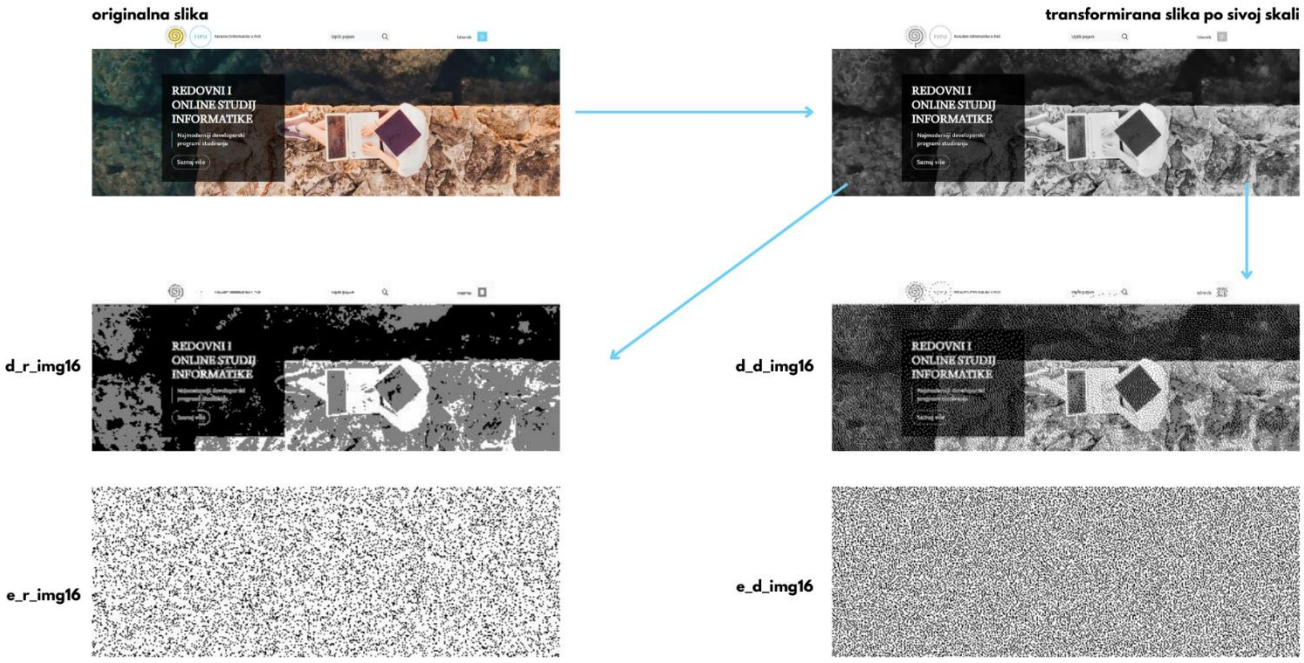
Slika 23. Vodeća slika po sivoj skali

- *d_r_im3* – dekriptirana slika smanjene palete boja
- *d_d_im3* – dekriptirana slika na kojoj je korišten Floyd-Steinbergov algoritam
- *e_r_im3* – enkriptirana slika smanjene palete boja
- *e_d_im3* – enkriptirana slika na kojoj je korišten Floyd-Steinbergov algoritam

```
import numpy as np
from PIL import Image
from cryptography.fernet import Fernet

# Generiranje novog enkripcijskog kljuca
encryption_key = Fernet.generate_key()
cipher_suite = Fernet(encryption_key)

GREYSCALE = True
img_name      =      r'C:\Users\almas\Desktop\Diplomski\Diplomski-rad\vodeca-
slika_grayscale.jpg'

# Otvaranje slike i provjera skale sive boje
img = Image.open(img_name)
width, height = img.size
new_width = 400
new_height = int(height * new_width / width)
img = img.resize((new_width, new_height), Image.LANCZOS)
```

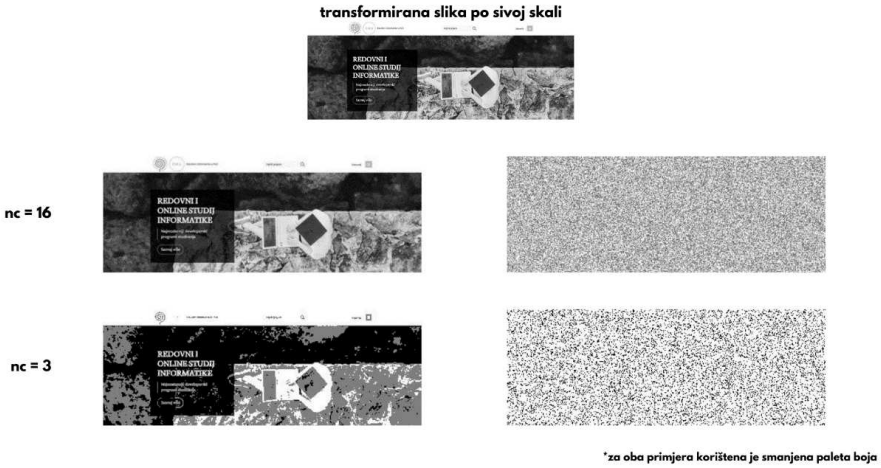
```
def get_new_val(old_val, nc):
    return np.round(old_val * (nc - 1)) / (nc - 1)
# Floyd-Steinbergov algoritam za normalizaciju vrijednosti piksela
def fs_dither(img, nc):
    arr = np.array(img, dtype=float) / 255

    for ir in range(new_height):
        for ic in range(new_width):
            old_val = arr[ir, ic].copy()
            new_val = get_new_val(old_val, nc)
            arr[ir, ic] = new_val
            err = old_val - new_val
            if ic < new_width - 1:
                arr[ir, ic+1] += err * 7/16
            if ir < new_height - 1:
                if ic > 0:
                    arr[ir+1, ic-1] += err * 3/16
                arr[ir+1, ic] += err * 5/16
                if ic < new_width - 1:
                    arr[ir+1, ic+1] += err / 16
    carr = np.array(arr/np.max(arr, axis=(0,1)) * 255, dtype=np.uint8)
    return Image.fromarray(carr)

# Funkcija za smanjenje broja boja u slici
def palette_reduce(img, nc):
    arr = np.array(img, dtype=float) / 255
    arr = get_new_val(arr, nc)
    carr = np.array(arr/np.max(arr) * 255, dtype=np.uint8)
    return Image.fromarray(carr)

# Iteracija kroz razlicite brojeve boja
for nc in (3,):
    print('nc =', nc)

encrypted_img_data = cipher_suite.encrypt(img.tobytes())
encrypted_img = Image.frombytes('L', img.size, bytes(encrypted_img_data))
dim = fs_dither(encrypted_img, nc)
dim.save(f'encrypted_fipu_bw-dimg-{nc}.jpg')

# Smanjenje palete boja na enkriptiranoj slici
rim = palette_reduce(encrypted_img, nc)
rim.save(f'encrypted_fipu_bw-rimg-{nc}.jpg')

# Dekripcija enkriptirane slike
decrypted_img_data = cipher_suite.decrypt(encrypted_img_data)
```

```
decrypted_img = Image.frombytes('L', img.size, bytes(decrypted_img_data))

decrypted_dim = fs_dither(decrypted_img, nc)
decrypted_dim.save(f'decrypted__fipu_bw-dimg-{nc}.jpg')

# Smanjenje palete boja na dekriptiranoj slici
decrypted_rim = palette_reduce(decrypted_img, nc)
decrypted_rim.save(f'decrypted_fipu_bw-rimg-{nc}.jpg')
```



Slika 24. Procesi enkripcije i dekripcije za vizualnu kriptografiju difuzije polutonskih pogrešaka (Floyd-Steinbergov algoritam)

Uz spomenuto, broj *3* mogao je biti postavljen na 2, 4, 8 ili 16 jer tim njime iskazujemo koliko različitih vrijednosti boja koristimo. Što je broj veći, to je slika „finija“ što dokazuje i slika 25.



Slika 25. Utjecaj promjene parametra broja boja u paleti na finoću slike

Uz sve pokazano, treba imati i na umu da postoje situacije kada slike koje koristimo možda nisu najpogodnije zbog primjerice svoje prozirne pozadine. Za sljedeći primjer, koristili smo logo iz zaglavlja stranice i metodom polutoniranja po sivoj skali dokazali blažu distorziju vidljivu i na slici 26:

Slika 26. Blaga distorzija originalne slike logoa obzirom na prozirnu pozadinu

Neovisno o spomenutom nedostatku, ovakva vrsta kriptografije korisna je obzirom na nisku složenost i sigurno dijeljenje polutonova s dobrom kvalitetom slike. Takav proces je vrlo „zahvalan“ u slučaju rekonstrukcije tajne slike. [26]

4.3. Vizualna kriptografija za više tajni

Treća vrsta, vizualna kriptografija za dijeljenje više tajni (eng. *visual cryptography for multiple secrets sharing*) shema je za $x \geq 2$ tajni tako da nijedna pojedinačna ne propušta tajne. Tajan x se može dobiti slaganjem jedne po jedne tajne. Donosi nekoliko shema, ali će zbog konciznosti biti predstavljene dvije osnovne i jedna kombinacijska.

Prva shema uključuje primjenu polinomno temeljene enkripcije i dekripcije pri čemu polinomno označava korištenje polinoma i matematičkih funkcija (zbrajanje i množenje) u svrhu šifriranja podataka. [27] Primjer koji se ovdje [28] spominje predlaže učinkovit, centraliziran tajni protokol dijeljenog praga (eng. *threshold shared secret protocol*) koji se temelji na Shamirovoj tehnici dijeljenja tajni i podržava autentifikaciju ključa korištenjem HMAC-a (eng. *Hashed Message Authenticate Code*) kojeg sam se dotakla i u *Gaming* potpoglavlju.

Predloženi protokol omogućuje generiranje glavnog tajnog ključa za grupu n entiteta i podjelu tog ključa na tajne udjele pri čemu se svaki dio sigurno distribuira svim članovima grupe. Nadalje, t od n entiteta mora kombinirati tajne udjele i obnoviti tajni ključ čije se prihvaćanje temelji na ispravnosti zaprimljenog HMAC potpisa. Za podrobnije shvaćanje ove teme, uvodimo polinome koji su u Shamirovom dijeljenju tajni zapisani kao:

$$f(x) = a_0 + a_1x^1 + a_2x^2 + a_3x^3 + a_{t-1}x^{t-1}\, mod(p)$$

Udjeli sudionika su zapisani kao koeficijenti u polinomu, a izabrani su nasumično. Vrijednost glavne dijeljene tajne razbijena na dijelove je:

- a_0 – vrijednost slobodnog koeficijenta
- $t - 1$ – stupanj polinoma koji indicira da je broj koeficijenta uvijek t

Dok je Lagrangeova interpolacija[12] za oporavak $f(x)$: y-koordinata točke na polinomu dobivena evaluacijom $f(x)$ što znači da je jedna točka na polinomu definirana pomoću:

$$(x, y = f(x))$$

[12] Koristi se za aproksimaciju funkcije temeljem niza poznatih vrijednosti i omogućuje stvaranje polinoma koji prolazi kroz zadane točke

Ukoliko je korištena spomenuta interpolacija, samo t bodova na stupnju $t-1$ je potrebno za rekonstrukciju. Iz toga slijedi da set $t-1$ udjela za $(x_0, y_0), (x_1, y_1), \dots, (x_{t-1}, y_{t-1})$ možemo zapisati kao Lagrangeovu bazu polinoma:

$$L_j(x) = \prod_{i=0, i\neq j}^{t-1} \frac{x - x_i}{x_j - x_i}$$

Iz koje možemo rekonstruirati $f(x)$:

$$f(x) = \sum_{j=0}^{t-1} y_j L_j(x)\, mod(p)$$

Iako mi marimo samo za vrijednost $f(0)$ koja je jednaka slobodnom koeficijentu iz $f(x)$, izračun može biti skraćen na:

$$f(0) = \sum_{j=0}^{t-1} \left(y_j \prod_{i=0, i\neq j}^{t-1} \frac{x_i}{x_i - x_j} \right) mod(p)$$

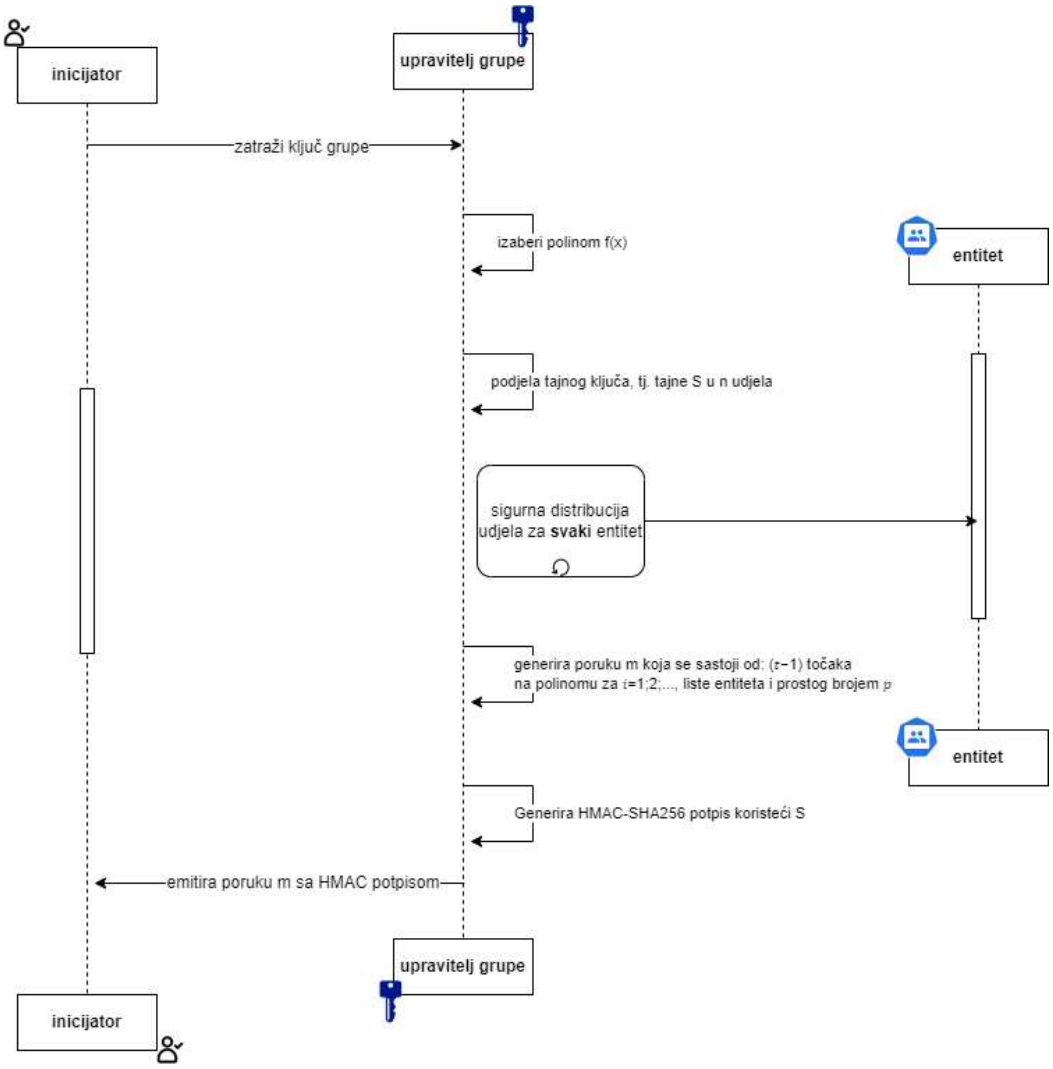
gdje $f(0)$ predstavlja originalan tajni ključ.

Glede generiranja ključa, predstavljen je protokol u kojem jedna osoba koja se smatra pouzdanom, npr. upravitelj grupe (UG) odabire glavni ključ za grupu i zatim ga dijeli na različite tajne dijelove koji se mogu sigurno distribuirati svim sudionicima. Kako bi se entitet „pretplatio“ na uslugu distribucije ključeva, mora se registrirati kod UG koji održava popis svih registriranih korisnika i uklanja one kojima je onemogućeno primanje grupne komunikacije. Postoje dvije vrste sigurnosnih protokola: distribuirani protokoli i centralizirani protokoli za upravljanje ključevima. Kod distribuiranih protokola, svaki entitet mora izračunati grupni ključ u stvarnom vremenu i podijeliti teret upravljanja ključem, troškove izračuna generiranja i komunikacije sa svakim članom grupe. Upravo time što se spomenuto raspoređuje na cijelu grupu, povećava sigurnost i toleranciju na greške. Centraliziranim protokolima, tj. generiranjem, distribucijom i ažuriranjem ključeva upravlja treća strana (eng. *third party*) što smanjuje opterećenje na spojene entitete.

U nastavku slijede 3 faze centraliziranog grupnog protokola ključa:

1. Faza generiranja ključa kao enumeracija prikazana je u dijagramu protokola na slici 27 gdje je:

- UG – upravitelj grupe
- *n* – veličina grupe
- *S* – tajna
- *t* – br. sudionika potreban za obnovu glavnog ključa
- *m* – minimalan broj za vrijednost ključa
- *p* – prost broj za definiranje razine sigurnosti nad poljem konačne veličine F_p
- *f(x)* – vrijednost polinoma s parametrima (*n, T, p, S*)
- vrijednost ključa mora biti između *m* i *p-1*

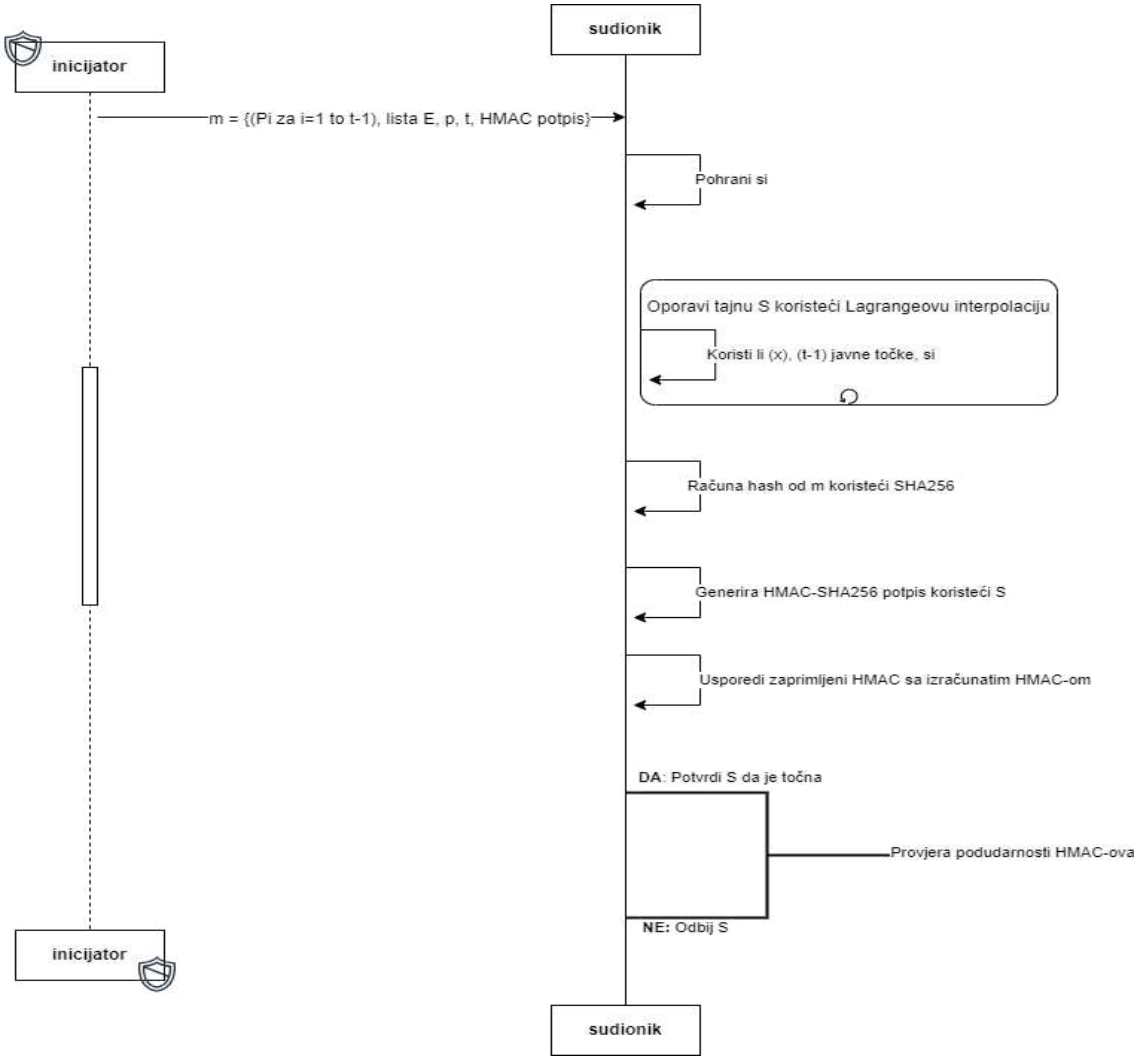


Slika 27. Generiranje ključa, autorski rad po uzoru na spomenuto istraživanje

2. Faza autentifikacije ključa

Za razliku od prethodnih protokola upravljanja ključevima koja koriste vrlo složene metode poput operacije s eliptičnim krivuljama i bilinearnog sparivanja, ovaj protokol koristi HMAC-SHA256 kako osigurao autentifikaciju poruka i integritet. HMAC će omogućiti i pošiljatelju i primatelju dijeljenje zajedničkog tajnog ključa za izračun potpisa koda nad prenesenom porukom. Na strani pošiljatelja, UG generira HMAC potpis koristeći generirani tajni glavni ključ *S* i jednosmjernu funkciju sažetka (eng. *one-way hash function*), zatim sažima poruku *m* koristeći SHA256 i računa HMAC potpis koristeći prethodno spomenuti tajni ključ. Nadalje, UG prenosi poruku generiranja ključeva *m* koja sadrži *t* – 1 javnih točaka povezanih sa HMAC potpisom kako bi omogućio autentifikaciju za sudionike.

3. Rekonstrukcija ključa

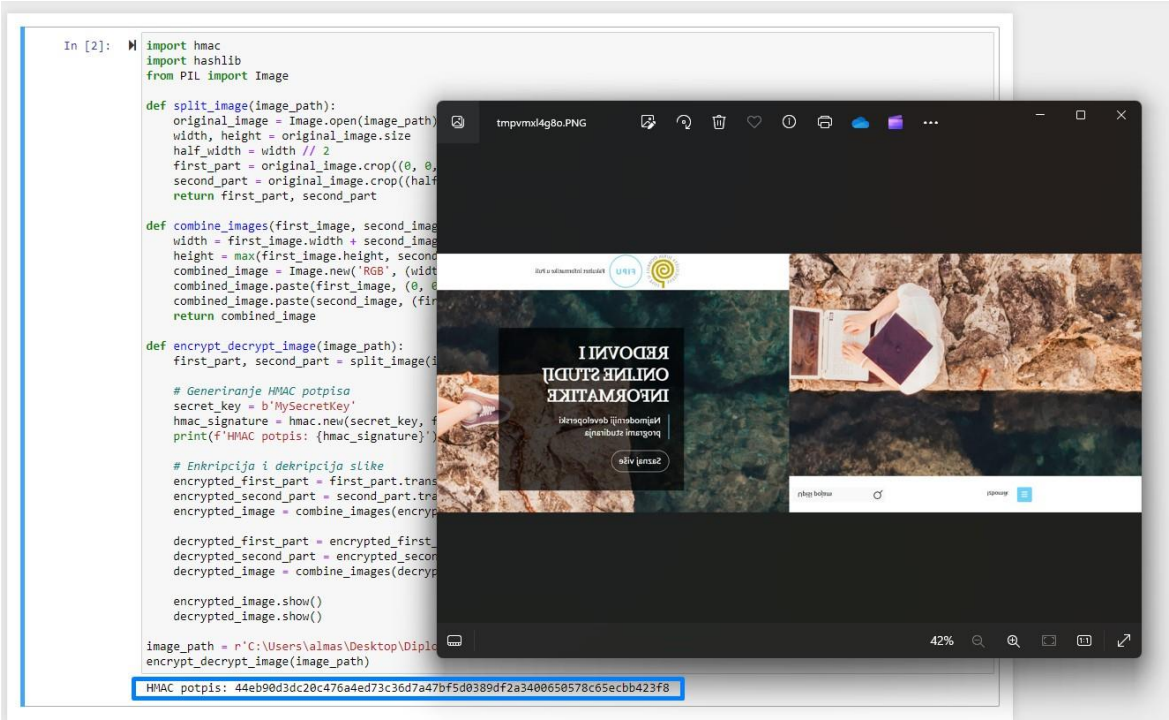


Slika 28. Rekonstrukcija ključa, autorski rad po uzoru na spomenuto istraživanje

Svime spomenutim se postiže bezuvjetna sigurnost i neprobojnost te idealna/savršena rekonstrukcija svih dijeljenih tajnih slika kao što je vidljivo na slici 29. Shema može uključivati i jednokratnu autentifikaciju za sve podijeljene tajne slike koristeći proširenu vizualnu kriptografiju koja je, zbog jednostavnosti, isključena iz niže priloženog koda.

```
import hmac
import hashlib
from PIL import Image

def split_image(image_path):
    original_image = Image.open(image_path)
    width, height = original_image.size
    half_width = width // 2
    first_part = original_image.crop((0, 0, half_width, height))
    second_part = original_image.crop((half_width, 0, width, height))
    return first_part, second_part

def combine_images(first_image, second_image):
    width = first_image.width + second_image.width
    height = max(first_image.height, second_image.height)
    combined_image = Image.new('RGB', (width, height))
    combined_image.paste(first_image, (0, 0))
    combined_image.paste(second_image, (first_image.width, 0))
    return combined_image

def encrypt_decrypt_image(image_path):
    first_part, second_part = split_image(image_path)

    # Generiranje HMAC potpisa
    secret_key = b'MySecretKey'
    hmac_signature = hmac.new(secret_key, first_part.tobytes() +
second_part.tobytes(), hashlib.sha256).hexdigest()
    print(f'HMAC potpis: {hmac_signature}')

    # Enkripcija i dekripcija slike
    encrypted_first_part = first_part.transpose(Image.FLIP_LEFT_RIGHT)
    encrypted_second_part = second_part.transpose(Image.FLIP_TOP_BOTTOM)
    encrypted_image = combine_images(encrypted_first_part,
encrypted_second_part)

    decrypted_first_part =
encrypted_first_part.transpose(Image.FLIP_LEFT_RIGHT)
```

```
    decrypted_second_part =
encrypted_second_part.transpose(Image.FLIP_TOP_BOTTOM)
    decrypted_image = combine_images(decrypted_first_part,
decrypted_second_part)
    encrypted_image.show()
    decrypted_image.show()

image_path = r'C:\Users\almas\Desktop\Diplomski\Diplomski-rad\vodeca-slika.jpg'

encrypt_decrypt_image(image_path)
```



Slika 29. Primjena vizualne kriptografije za više tajni na primjeru vodeće slike mrežne stranice FIPU

Druga shema koristi ranije spomenuti pristup polutoniranja. Tajni binarni piksel kodira se u niz/polje subpiksela koji se zovu „polutonske ćelije“ u svakom udjelu. Takav pristup omogućuje rekurzivno skrivanje [29] manjih tajni u udjelima većih čime se povećavaju informacije svakim novim udjelom.

Posljednja shema je kombinacija koju ova vrsta vizualne kriptografije dozvoljava koristeći druge tehnike poput npr. steganografije. Svodi se na već utemeljenu sigurnost koja ne propušta nekvalificirane sudionike (svaki sudionik koji nema mogućnost rekonstrukcije originalne tajne slike ni pristup ključnim dijelovima slike koji su potrebni za dešifriranje tajnih informacija) niti im daje informacije za rekonstrukciju tajnih informacija. [30]

Sve spomenute tehnike i sheme oslanjaju se na veliku fleksibilnost u broju udjela. Tajna se poruka može podijeliti na bilo koji broj udjela, ovisno o zahtjevima i sigurnosnim potrebama. To za sobom „povlači“ činjenicu primjene u različitim područjima gdje se ponajprije ističe zaštita autorskih prava koja su i sama posljedica dijela istraživačkog naslova; odnosno digitalnog sadržaja.

4.4 Proširena vizualna kriptografija za slike

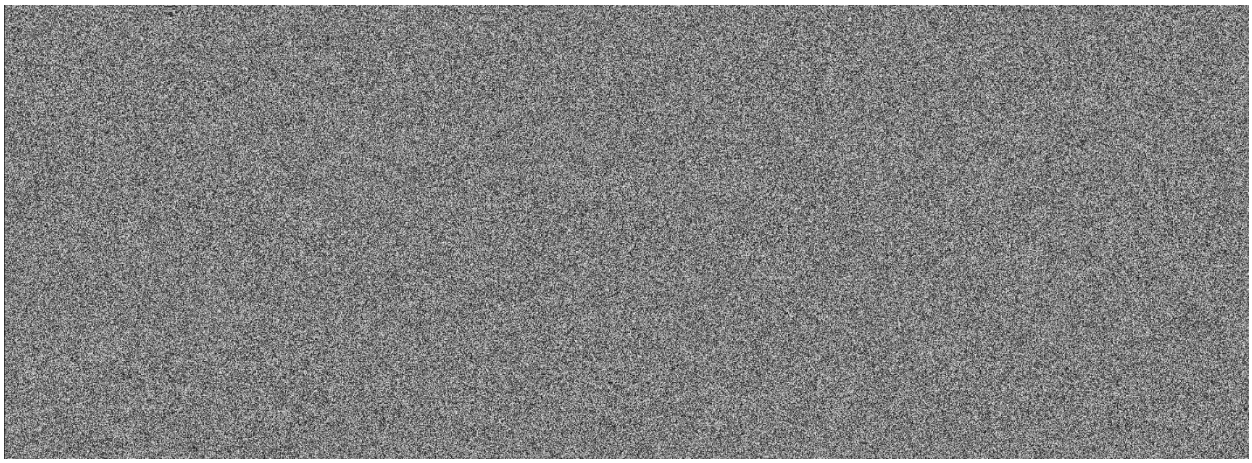
Najsloženija vrsta vizualne kriptografije, glede rada, jest proširena vizualna kriptografija gdje proširena označava mogućnost ispisa bolje kvalitete slike jer se tajna poruka distribuira na više dijelova. Prateći rad [31], algoritam koristi DST (eng. *Discrete Shearlet Transform*) koji predstavlja vrstu transformacije i razdvaja informacije u slici na različite skale, npr. kanali slike. Spomenuto pruža dodatne, naprednije tehnike dijeljenja informacija i postizanja veće sigurnosti, npr. steganografija[13] ili u enkripciji.

```
import numpy as np
from PIL import Image
from scipy.fftpack import dst, idst, fftshift, ifftshift

def split_image(image_path):
    original_image = Image.open(image_path)

    image_array = np.array(original_image.convert('L'))

    # Primjena DST na sliku
    dst_image = dst(image_array, axis=0)

    # Primjena FFTShift na sliku
    shifted_image = fftshift(dst_image)

    width, height = shifted_image.shape
    half_width = width // 2

    # Prvi dio transformirane slike
    first_part = shifted_image[:half_width, :]

    # Drugi dio transformirane slike
    second_part = shifted_image[half_width:, :]

    return first_part, second_part
```

[13] Steganografija je tehnika skrivanja tajne poruke unutar nevidljivog medija kako bi se ostvarila tajnost komunikacije (npr. LSB (*Least Significant Bit*) metoda u slikama – metoda zamjene najmanje značajnih bitova u slikama koji ne utječu na percepciju slike s bitovima tajne poruke)

```
def combine_images(first_image, second_image):
    width = first_image.shape[1]
    height = first_image.shape[0] + second_image.shape[0]
    combined_image = np.zeros((height, width), dtype=np.float64)
    combined_image[:first_image.shape[0], :] = first_image
    combined_image[first_image.shape[0]:, :] = second_image

    return combined_image

def encrypt_decrypt_image(image_path):
    first_part, second_part = split_image(image_path)

    # Rekonstrukcija transformiranih dijelova slike
    reconstructed_first_part = ifftshift(first_part)
    reconstructed_second_part = ifftshift(second_part)

    # Inverzni DST na transformirane dijelove slike
    reconstructed_first_part = idst(reconstructed_first_part, axis=0)
    reconstructed_second_part = idst(reconstructed_second_part, axis=0)

            reconstructed_image      =      combine_images(reconstructed_first_part,
reconstructed_second_part)
    reconstructed_image = Image.fromarray(reconstructed_image.astype(np.uint8))
    reconstructed_image.show()

image_path = r'C:\Users\almas\Desktop\Diplomski\Diplomski-rad\vodeca-slika.jpg'

# Enkripcija i dekripcija slike
encrypt_decrypt_image(image_path)
```

Slika 30 prikazuje enkriptiranu vodeću sliku u kojoj se uočavaju drastičnije razlike obzirom na pristup XOR operacije po kanalima, dok je dekriptirana slika u potpunosti očuvana.



Slika 30. Enkriptirana vodeća slika uz pomoć proširene vizualne kriptografije za fotografije u boji

Shema po kojoj proširena vizualna kriptografija funkcionira bazira se na podjeli vodeće slike na 3 kanala, npr. RGB gdje 0 predstavlja crvenu, 1 zelenu, a 2 plavu vrijednost, a sama važnost je na uvođenju značajne slike (eng. *meaningful image*) kao zasjenjujuće slike (eng. *shadow image*).

Pri čemu je:

- **značajna slika** (eng. *meaningful image*) – originalna slika koja se izabire kao ona gdje skrivamo tajnu (enkriptiramo)
- **zasjenjujuća slika** (eng. *shadow image*) – slika na folijama koja predstavlja dio iz kojeg je nemoguće saznati ikakvu tajnu informaciju bez drugih udjela

Kao rezultat toga dijeljena (tajna) slika može biti obnovljena iz bilo kojeg „kvalificiranog“ skupa bez ikakvog traga sjenovite slike, ali uz ograničenje da „zabranjeni“ skup nema nikakve informacije o tajnoj slici. Sjenovite slike su značajne tako da svaki sudionik može prepoznati sliku na folijama.

Proširena vizualna kriptografija koristi značajne udjele i prepoznatljive slike za razliku od „jednostavne“ VK[14] koja generira nasumične šumove kao udio.

[14] VK = vizualna kriptografija

Da bi to sve bilo izvedivo potrebna su 3 uvjeta:

1. **uvjet kontrasta** (eng. *contrast condition*) – bilo koji kvalificirani skup može rekonstruirati tajnu sliku pri čemu se isti odvija naslagivanjem folija; uz uvjet da je kontrast dostatan i da slika ima veliku količinu detalja bez snažnih šumova
2. **uvjet sigurnosti** (eng. *security condition*) – nijedan zabranjeni skup nema informacije o slici
3. **„produženi" uvjet** (eng. *extended condition*) – implicira da su sjenaste slike i dalje značajne nakon enkriptiranja originalnih

Posljednji uvjet dolazi uz jedno ograničenje, a tiče se kontrasta. Nemoguće je simultano povećavati kontrast sjenaste i rekonstruirane slike. Iz tog razloga proizlazi i činjenica da je za proširenu vizualnu kriptografiju potrebno, očekivano, više piksela.

Jednostavnost i dostupnost digitalnih kamera uvelike olakšava proces „nabavljanja" slika kontinuiranog tona. Ipak, slika koju čovjek percipira mora biti pretvorena u što sličniju binarnu kako bi ju bilo moguće procesuirati. Algoritam koji pomaže u tome spomenut je i ranije, a naziva se polutoniranje te nudi:

- **uzorak gustoće (eng. *density pattern*)** – oslanja se na korištenje *l* broja subpiksela koji predstavljaju svaku vrijednost piksela. Ova metoda se ne smatra najprikladnijom zbog, zvuči kontradiktorno, ali mana koje su ujedno i prednosti; počevši od kvalitete slike i količine gustoće. Estetski gledano, nedovoljno složen uzorak sliku čini kvalitetnijom i vizualno privlačnijom, ali zato i podložnijom sa sigurnosnog aspekta. Pretjerana gustoća uzorka može degradirati samu sliku i utjecati na složenost implementacije što rezultira dodatnom obradom slike.
- **enkodiranje šuma (eng. *noise-encoding*)** – pomaže u poboljšanju kvalitete slike. Dodaje se u ranoj fazi digitalnog polutoniranja kao tzv. nasumični šum (eng. *random noise*), odnosno bijeli šum (eng. *white noise*)
- **uređeno podrhtavanje (eng. *ordered dither*)** – generira binarnu sliku usporedbom piksela izvorne slike kontinuiranog tona s vrijednostima matrice da bi se postigao efekt simulacije dubine boje ili nijanse

- **difuzija pogreške (eng**. ***error diffusion*****)** – prethodno opisano načelo; nedostatak propisno raspršenih tajnih informacija u slikama
- **iterativne metode i metode bazirane na traženju (eng**. ***iterative and search-based methods*****)** – iterativnim koracima ili pretragom postižu se optimalna rješenja

Zaključno, proširena vizualna kriptografija pruža brojne mogućnosti glede integracije s drugim sigurnosnim tehnikama, a uz to poboljšava kvalitetu i sigurnost dijeljenih slika te obnovljenih tajnih. Primjene ovakve vizualne kriptografije su različite uključujući biometrijsku sigurnost, sigurnost medicinskih podataka i prijenos istih; što će kasnije biti i detaljnije objašnjeno.

5. Primjeri i primjene vizualne kriptografije

5.1. QR kodovi

Definicija 1. *Brzi odgovor (eng. Quick response, tj. QR) vrsta je popularnog dvodimenzionalnog barkoda koji se sastoji od manjih crnih kvadrata unutar većeg bijelog kvadrata na bijeloj pozadini.*

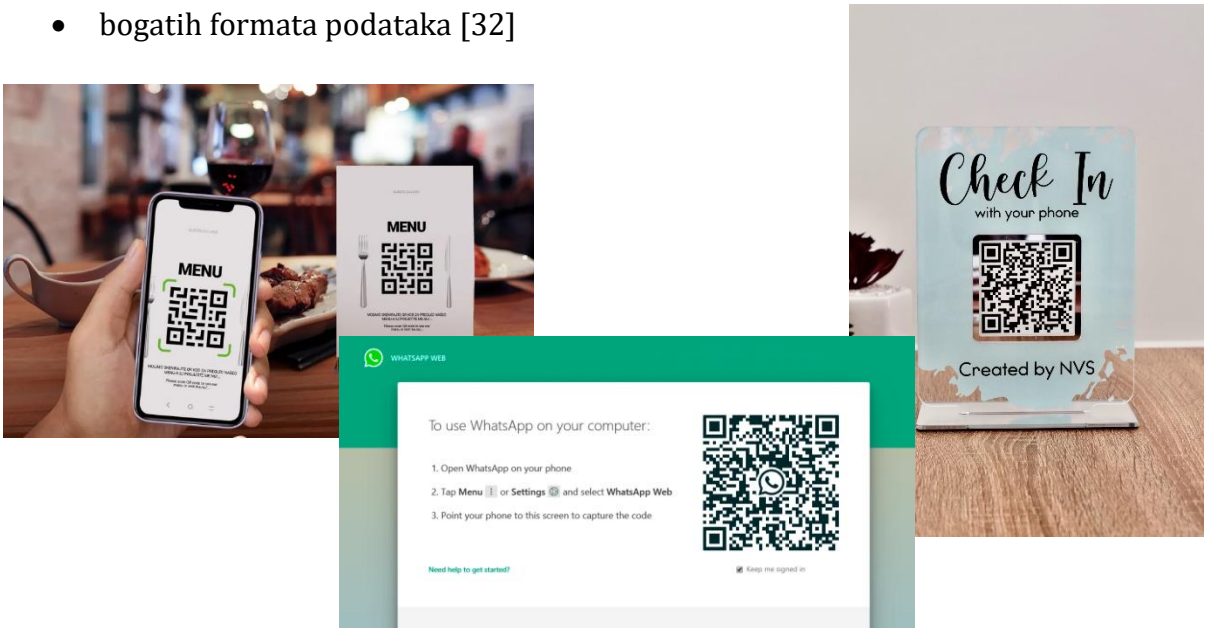
Kategorija kojoj ovakva primjena pripada jest kod obzirom da predstavlja, tj. skriva podatke na vizualan način. Ključem se smatraju sva pravila (razine ispravka pogrešaka) i konfiguracije (čitljivost pri uvjetima smanjene svjetline, oštećenjima ili blizine objekta koji ga skenira) koja određuju strukturu i sadržaj samog koda.

Proces enkripcije: kodiranje informacija/sadržaja poput: URL-a, teksta, broja telefona i binarnih podataka) pomoću crnih (tamnih) i bijelih (svijetlih) kvadrata

Proces dekripcije: skeniranje sa čitačem ili kamerom

Uz to, QR kod strojno je čitljiva optička oznaka s prednostima poput:

- brzog čitanja – slika 31 prikazuje razne mogućnosti koje QR kod pruža (npr. skeniranje i pregled jelovnika, beskontaktna prijava dolaska u apartman/hotel, prijava u web aplikaciju za korištenje računalne verzije WhatsApp-a)
- mogućnostima korekcije pogrešaka
- bogatih formata podataka [32]



Slika 31. Primjene QR koda u svrhu brzog čitanja

Zahvaljujući razvoju mobilnog interneta, QR kod nalazi svoju široku primjenu u prijenosu složenih digitalnih informacija u fizički svijet, primjerice za plaćanje gdje sustavi koriste mobilne aplikacije i servere za plaćanje koji koriste vizualnu kriptografiju sigurnih transakcija [33].

Vizualna kriptografija u QR kodovima je tehnika koja kombinira prednosti moderne biotehnologije sa algoritmima informacijske sigurnosti radi poboljšanja zaštite privatnosti i sigurnog prijenosa tajnih informacija [34]. Jedna metoda vizualne kriptografije u QR kodovima uključuje generiranje vizualno privlačnih kodova za prijenos značajnih udjela. Izvorna tajna slika obrađuje se vodenim žigom, poput logotipa autorskih prava ili potpisa, a zatim se vrši polutonska obrada vodenim slikama kako bi se ograničilo proširenje piksela. Polutonirana slika se zatim dijeli na dva udjela [35]. Ovakva generalizacija moguća je ponajprije zbog izgleda QR koda koji je sličan principu vizualnog dijeljenja tajni budući da su oba crno-bijele (binarne) slike.

QR kodovi se također koriste za autentifikaciju e-glasovanja i digitalne žigove. [36] Jednostavnost „leži“ u ljudskom vizualnom sustavu koji može otkriti tajnu sliku stapanjem, a kada je dostupno računanje, može otkriti i sliku bolje vizualne kvalitete na temelju već ranije spomenute XOR operacije. Da bi uvjeti korekcije pogrešaka bili zadovoljeni, veća tajna slika mora generirati više slika udjela. QR kodovi se mogu koristiti kao sredstvo distribucije i ugrađivanja tajnih informacija u sam vizualni kod. Upotreba takvih kodova u shemi vizualnog dijeljenja tajni, glavni je prijedlog kako bi se riješili sigurnosni problemi poput curenja informacija i manipulacije podacima što je opisano mehanizmom niže. [37]

QR kod sa skrivenim informacijama uzima se kao originalna tajna slika, koja koristeći posebnu enkripcijsku metodu pseudo-nasumičnom matricom, u kombinaciji sa algoritmima vizualne kriptografije generira dvije dijeljene slike. Cijeli proces svediv je na tek nekoliko koraka:

1. prikupljanje enkodiranih matrica C_0 i C_1 – po svojoj vrsti su *boolean*, a predstavljaju crni i bijeli piksel originalne tajne slike
2. generiranje pseudo-nasumičnih matrica – takva matrica je iste veličine kao originalna slika pri čemu svaka vrijednost odgovara matrici C_0 i C_1 redom

Osnovna matrica u C_1 je XOR-ana sa osnovnom matricom u C_0 i matricom gdje su sve jedinice

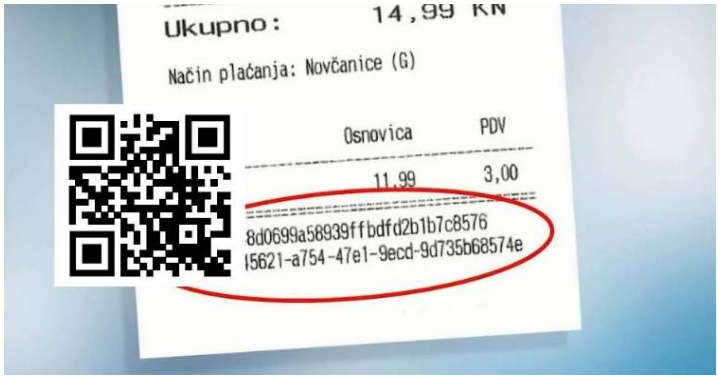
3. odabir osnovne matrice – matrica piksela dijeljene slike osnovna je matrica odabrana iz C_0 ili C_1, ali odabrano pravilo određeno je uz pseudo-nasumičnu matricu

U slučaju bijelog piksela: pozicija u tajnoj slici mapira se na odgovarajuću poziciju u pseudo-slučajnoj matrici, a zatim se odgovarajuća osnovna matrica odabire iz C_0

U slučaju crnog piksela: cijeli postupak ostaje gotovo isti osim što se osnovna matrica izabire iz C_1, (umjesto C_0) prema vrijednosti u pseudo-slučajnoj matrici.

4. rekonstruirana tajna slika – bijeli ili crni piksel u originalnoj tajnoj slici predstavljen je jednim potpikselom [38]

Dijeljenje slike generirane u ovom podsustavu su povezane pseudo-slučajnom matricom. Ako napadač i dobije osnovnu matricu, ne može doći do tajnih informacija. Ovime se osigurava siguran prijenos tajnih informacija i rješava problem jednostavne autentifikacije u različitim primjenama. Integracijom spomenutog kroz korištene sustave povećava se sigurnost distribucije tajnih podataka, a posljedično i poboljšavaju sustavi poput primjerice plaćanja. Primjer jednog vidljiv je na slici 32 koja prikazuje fiskalizirani hrvatski račun sa integriranim kodom.



Slika 32. Fiskalni račun sa integriranim QR kodom

Najnoviji primjer integracije QR koda na hrvatskom tržištu su studentske iksice koje se svojim unificiranim izgledom ne razlikuju na razini svih sveučilišta Hrvaske.

Osim taktilnih oznaka za slijepe i slabovidne, dodan je ESI (europski studentski identifikator) u obliku QR koda (jedinstven za svakog studenta i stoga je nasumično generiran na priloženoj slici). Nova i sigurnija tehnologija uz beskontaktni čip omogućava brojne pogodnosti od jednostavnijeg korištenja prijevoza i manje administrativne gnjavaže do ulaza u studentske prostorije i već poznatog korištenja u studentskom restoranu. Ono što Ministarstvo znanosti i obrazovanja najviše ističe jest „sigurnija kriptografija“ koja jamči najveću razinu zaštite podataka.

Slika 33. Nova studentska iksica u Hrvatskoj

Poznati primjeri ostalih barkodova su:

- UPC (*Universal product code*) – barkod koji se koristi za označavanje robe u trgovinama; varira između 12 i 13 znamenki
    - EAN (*European article number*) – europska inačica UPC-a koja se također sastoji od 12-13 znamenki (dolazi u izvedenicama kao što je: DAN – interno se koristi u pojedinim drogerijama, npr. dm).
- 2D barkod – najčešći je primjer u kućanstvu ako se uzme u obzir da je vidljiv na dnu svakog računa. Kao grafički prikaz, najčešće skeniranjem kroz mobilnu aplikaciju bankarstva izlistava: IBAN, model plaćanja, poziv na broj, opis i vrstu plaćanja te iznos za koji se tereti osobu koja izvodi plaćanje.

5.2. Autentifikacijski procesi i 2FA (eng. *two-factor authentification*)

Definicija 2. *2FA ili dvofaktorska autentifikacija sigurnosni je mehanizam koji od korisnika iziskuje dva različita tipa dokaza u svrhu verifikacije identiteta.*

2FA je jedan od načina autentifikacije, tj. sigurnosnog procesa potvrde identiteta predmeta interakcije u informacijskoj mreži pomoću jedinstvenih atributa. Nažalost, pokazalo se da je većina informacijskih sigurnosnih incidenata uzrokovana zbog korištenja samo jednog faktora prijave [39].

Najlakši način za „popravak" dodavanje je još jednog sigurnosnog sloja što rezultira 2FA. U ovom procesu autentifikacije, ključevi su kombinacije faktora koje korisnik pruža u svrhu potvrde identiteta, a najčešće ovo uključuje kombinaciju nečeg što korisnik zna (npr. lozinka) s nečim što korisnik posjeduje (npr. fizički token generator ili biometrijska karakteristika o kojoj će biti riječ kroz sljedeću cjelinu).

Proces enkripcije: generiranje jednokratnih lozinki ili tokena

Proces dekripcije: verifikacija jednokratnih lozinki ili tokena kako bi se potvrdio pristup

Osnovni primjeri su [40]:

- **2FA programi; klasificirani autentifikator** od kojih razlikujemo brojne poput:
    - *1Password* – preporuka je za pojedince koji imaju veliki broj profila s različitim lozinkama
    - *Google Authenticator*, *Microsoft Authenticator* – najčešće korišteni primjeri u većim poduzećima ili industrijama
    - *Twilio Authy* – za korisnike Apple Watcha i ostalih pametnih satova koji imaju mogućnost zaključavanja uređaja

- PingID – prikazan na slici 34, koristi se u poslovne svrhe za prijavu u radno okruženje koje pruža klijent. Korisnik, u ovom slučaju ja, moram znati korisničko ime i lozinku sustava u koji se prijavljujem, a mobilni uređaj mi „odašilje“ šest nasumično generiranih brojeva koje upisujem kao drugi korak autentifikacije. Tek kad se sva tri parametra poklope, pristup je odobren.

Slika 34. PingID kao primjer 2FA; autorska arhiva

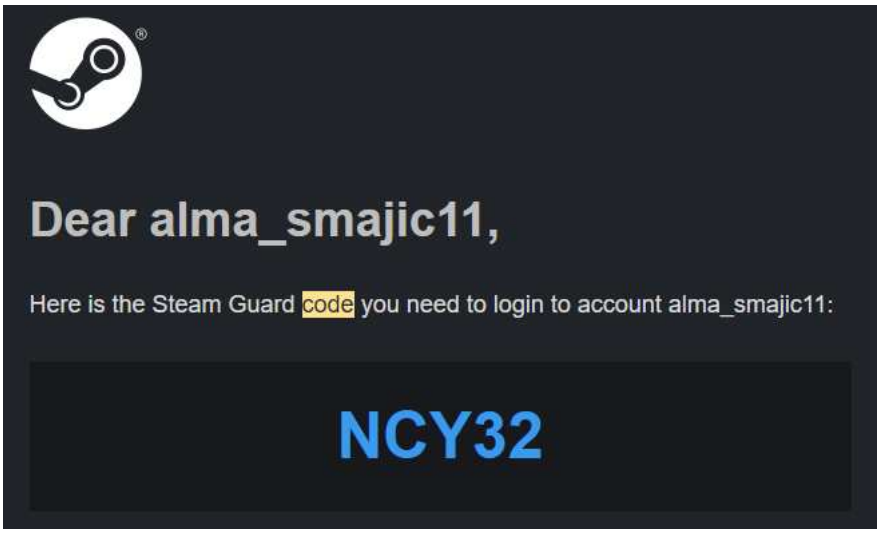
- **OTP (*one-time password*) token; hardverski generatori lozinki** – npr. u aplikaciji mobilnog bankarstva pri autorizaciji pojedinih dijelova/transakcija; vidljivo na slici 35

Slika 35. OTP Token unutar m-Zaba aplikacije; autorska arhiva

- **slanje jednokratne lozinke SMS-om** – npr. pri kreaciji novog BlaBlaCar profila što prikazuje slika 36

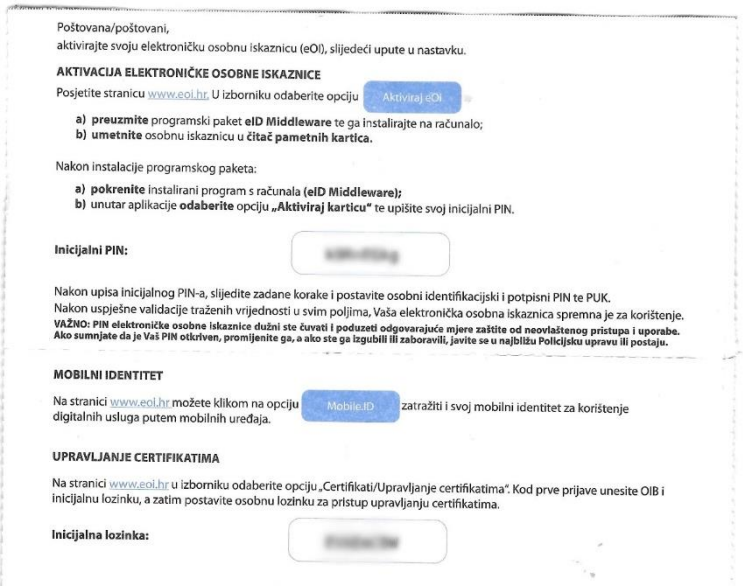
Slika 36. BlaBlaCar jednokratni kod za potvrdu pri kreaciji profila; autorska snimka zaslona

- **slanje privremenog koda na mail adresu** – npr. prilikom prijave u *Steam* aplikaciju kao na slici 37



Slika 37. Privremeni kod za prijavu u Steam aplikaciju, autorska arhiva

- **jednokratna lozinka na papiru (printabilan skup lozinki)** – npr. lozinke koje:
    - MUP izdaje građanima prilikom izrade novog oblika elektroničke osobne iskaznice (eOI) uz osobni primjer vidljiv na slici 38



Poštovana/poštovani,
aktivirajte svoju elektroničku osobnu iskaznicu (eOI), slijedeći upute u nastavku.

AKTIVACIJA ELEKTRONIČKE OSOBNE ISKAZNICE

Posjetite stranicu www.eoi.hr. U izborniku odaberite opciju Aktiviraj eOI.

a) **preuzmite** programski paket **eID Middleware** te ga instalirajte na računalo;
b) **umetnite** osobnu iskaznicu u **čitač pametnih kartica.**

Nakon instalacije programskog paketa:

a) **pokrenite** instalirani program s računala **(eID Middleware);**
b) unutar aplikacije **odaberite** opciju **„Aktiviraj karticu"** te upišite svoj inicijalni PIN.

Inicijalni PIN:

Nakon upisa inicijalnog PIN-a, slijedite zadane korake i postavite osobni identifikacijski i potpisni PIN te PUK.
Nakon uspješne validacije traženih vrijednosti u svim poljima, Vaša elektronička osobna iskaznica spremna je za korištenje.
VAŽNO: PIN elektroničke osobne iskaznice dužni ste čuvati i poduzeti odgovarajuće mjere zaštite od neovlaštenog pristupa i uporabe. Ako sumnjate da je Vaš PIN otkriven, promijenite ga, a ako ste ga izgubili ili zaboravili, javite se u najbližu Policijsku upravu ili postaju.

MOBILNI IDENTITET

Na stranici www.eoi.hr možete klikom na opciju MobileID zatražiti i svoj mobilni identitet za korištenje digitalnih usluga putem mobilnih uređaja.

UPRAVLJANJE CERTIFIKATIMA

Na stranici www.eoi.hr u izborniku odaberite opciju „Certifikati/Upravljanje certifikatima". Kod prve prijave unesite OIB i inicijalnu lozinku, a zatim postavite osobnu lozinku za pristup upravljanju certifikatima.

Inicijalna lozinka:

Slika 38. Jednokratne lozinke na papiru (eOI)

    - m-zaba (Zagrebačka banka) dodjeljuje pri postavljanju mobilnog bankarstva[15]

U navedenim primjerima, vizualna kriptografija se može iskoristiti kao jedan od faktora autentifikacije. Novi način provjere identiteta uključuje grafičku lozinku i primjenu vizualne kriptografije u kombinaciji sa *Twofish* enkripcijskim algoritmom – simetrični ključ s blokom od 128 bitova. Šifriranje se provodi jednostavnim preklapanjem općih slika i ne zahtijeva izračune kao logički izrazi. Na taj način sustav provjerava korisnika putem neredoslijedne grafičke lozinke (eng. *disorganized graphical password*). Za početak, ugrađena je šifrirana ključna riječ koja se u usporedbi sa alfanumeričkom lozinkom mora podudarati i sa redoslijedom grafičke lozinke i sa šifriranom ključnom riječi u grafičkoj lozinki. Kako je ključ šifriran pomoću *Twofish*-a ugrađenog u sliku, eliminirana je mogućnost predviđanja algoritma šifriranja za uzastopno hakiranje. [41]

[15] Papir se zbog sigurnosnih razloga odmah uništava stoga ne postoje vizualni primjeri kao za ostale primjere

Iako na prvu zvuči malo kompleksnije, iz istog proizlaze veliki benefiti:

1. poboljšanje sigurnosti dodatnim slojem – ako napadač dobije pristup na jedan faktor (npr. lozinku) i dalje su mu potrebni vizualni udjeli za uspješnu autentifikaciju
2. korisnička jednostavnost – korisnici mogu vrlo jednostavno zapamtiti i prepoznati vizualne uzorke za sliku, što cijeli autentifikacijski proces čini intuitivnijim i praktičnijim

Zaključno, vizualna kriptografija obećavajuća je tehnika za poboljšanje sigurnosti i korisnosti dvo-faktorske autentifikacije. Korištenjem vizualnih informacija i tajnog dijeljenja, daje dodatni sloj zaštite i jednostavnosti upotrebe (eng. *user-friendly*) pri prijavi. Trenutna istraživanja u ovom polju, poput onog iz 2022. (Abapour i Ebadpour [42]), ciljaju razviti robusnije i efikasnije algoritme. Spomenuti dvojac tako je predložio algoritam koji koristi slojevitu arhitekturu (eng. *layered architecture*) i adresirao svoju metodu; decentralizirana metoda simetrične vizualne kriptografije temeljena na rešetki (eng. *decentralized lattice-based method for visual symmetric cryptography*) kao NP-težak problem.

5.3. Vodeni žigovi (eng. *watermarks*)

Definicija 3. *Digitalni vodeni žig je proces ugrađivanja poluvidljive ili nevidljive digitalne informacije (tekst, logotip, uzorak) u multimedijske podatke (npr. pozadina dokumenta ili slika) bez izmjene originalne slike*.

Kategorizira se kao kriptosustav jer postoji otvoreni tekst koji se šifrira, šifrat te skup ključeva za koje se smatra da su to informacije ili elementi umetnuti u dokument ili sliku.

Korištene metode se prilagođavaju ovisno o tome gdje se žig umeće pa tako razlikujemo:

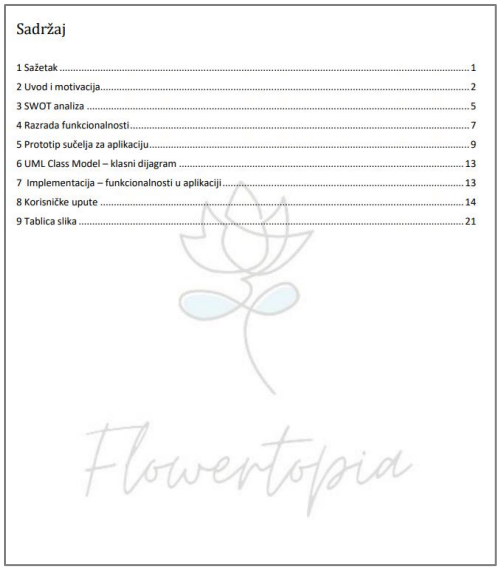
1. slikovne – transparentne ili poluvidljive slike koje se preklapaju s originalnom slikom ili dokumentom
2. tekstualne – skrivena tekstualna poruka koja se umeće u pozadinu dokumenta
3. kombinirane – kombinacija slike i teksta za identifikaciju

Kao u i prethodne dvije kategorije, ovdje razlikujemo:

Proces enkripcije: umetanje netom spomenutih elemenata na teško primjetan način ili takav način da se teško kopira

Proces dekripcije: identifikacija vodenog žiga u svrhu provjere autentičnosti dokumenta/slike

Svrha vodenih žigova pružanje je zaštite autorskih prava i utvrđivanje vlasništva nad slikama, primjerice slika 39 utvrđuje autorsko djelo uz prisustvo vodenog žiga u projektnoj dokumentaciji realiziranoj u sklopu kolegija *Izrada informatičkih projekata*.



Slika 39. Primjer vodenog žiga u dokumentaciji projekta; autorska arhiva (2023.)

Razlikuju se 3 kategorije vodenih žigova:

Prva kategorija

- vidljivi – dizajnirani tako da ih promatrač jednostavno vidi, vlasnik identificira, ali žig kao takav ne smije utjecati na sadržaj slike
- nevidljivi – neprimjetni u „normalnim“ uvjetima promatranja i koriste se za skrivanje podataka te steganografiji. Ovdje se također primjenjuje tehnika najmanje značajnog bita u kombinaciji sa kompresijom obzirom da su navedene tehnike najmanje primjetne ljudskom oku.

Druga kategorija

- fragilni (lomljivi) – dizajnirani su tako da se „slome“ pod najmanjom promjenom slike. Takav žig mora biti sposoban detektirati signal promjene, gdje se on točno dogodio, a ako je moguće i stanje prije promjene. Ovo je pronašlo svoju primjenu u provjeri autentičnosti dokumen(a)ta.
- robusni – dizajn im trpi višestruke napada procesiranja (npr. kompresija ili reskaliranje) stoga se njih stavlja na fizički/digitalni dokument.

Treća kategorija

- slijepi – izvršavaju provjeru oznake bez upotrebe izvorne slike
- neslijepi – svi ostali; oslanjaju se na originalni žig
- poluslijepi – koriste popratne informacije i/ili originalni žig

Posljednje prije povezivanja cjelokupnog pojma vodenog žiga s vizualnom kriptografijom slijedi pregled „zahtjeva“ za idealni sustav:

1. neprimjetnost – ako sustav izobliči sliku do te mjere da postaje beskorisna ili izrazito „ometena“, žig neće ispuniti svoju glavnu svrhu. U idealnim uvjetima, slika sa vodenim žigom bi trebala biti neodvojiva od originala.
2. iznimna robusnost – predstavlja otpornost na izobličenja koja nastaju tijekom normalne upotrebe („nehotični napad“ – npr. kompresija koja je mogla nastati prilikom rezanja/promjene veličine slike) ili namjernog pokušaja uklanjanja žiga

(„zlonamjerni napad“ – napadač pokušava onesposobiti žig dodavanjem geometrijskih oblika ili dodavanjem šuma).

3. kapacitet i brzina – kapacitet varira od jednog bita do više odlomaka teksta, ali mora dozvoliti ugradnju korisne količine informacija. Brzina je važna samo u aplikacijama koje zahtijevaju ugradnju u stvarnom vremenu.

Ideju korištenja vizualno-kriptografske tehnike za označavanje vodenim žigom, Hwang [43] je predstavio 2000. godine. Predložio je shemu u kojoj se određeni broj piksela originalne slike nasumično odabire pritom koristeći tajni ključ. Tada se najznačajniji bit svakog odabranog piksela s binarnim vodenim žigom koristi za generiranje slika vlasnika. Sve ideje i prijedlozi su se dalje samo oslanjali na spomenuto što je dalo temelje za tehnike bazirane na [44]:

- DWT (eng. *discrete wavelet transform*) – razlaže sliku na različite komponente koje predstavljaju frekvencijske pojaseve
- SIFT (eng. *scale invariant feature transform*) – algoritam u računalnom vidu za detekciju i opisivanje karakterističnih točaka u digitalnim slikama
- SVD (eng. *singular value decomposition*) – matematička tehnika korištena u linearnoj algebri i numeričkoj analizi. Ujedno je i faktorizacija koja predstavlja matricu koja proizlazi iz umnoška 3 jednostavnije matrice:
    - U – ortogonalna matrica (matrica kojoj je transponirana matrica jednaka vlastitoj inverznoj matrici)
    - D – dijagonalna matrica (tip matrice kojoj su svi elementi izvan glavne dijagonale iznose nula)
    - V^T – transponirana ortogonalna matrica V

To znači da za razliku od tradicionalnih tehnika vodenih žigova gdje se vodeni žig ugrađuje u digitalnu sliku, vodeni žig temeljen na vizualnoj kriptografiji, konstruira neovisne glavne udjele za autore prema originalnoj slici. Ovaj pristup omogućuje ugradnju vodenog žiga bez modifikacije originalne slike i omogućuje autoru otkrivanje žiga pokazivanjem vlastitih udjela u slučaju piratstva.

Osim što se jednostavno repliciraju, trajno označavaju podatke, daju identične kopije digitalnih podataka te nude sigurnu i pouzdanu metodu za zaštitu prava digitalnih slika bez ugrožavanja kvalitete. Novo-predložene tehnike pokazale su otpornost na razne napade, uključujući rotaciju i skaliranje, poboljšale sigurnosnu snagu vizualne kriptografije i osigurale integritet podataka. Jedino što preostaje jest uvesti standard za razvoj i implementaciju u upravljanje digitalnim pravima.

Mehanizmi i algoritmi na primjeru reverzibilnog umetanja vodenog žiga

Kada je efekt distorzije manje važan, za zaštitu autorskih prava, umjesto digitalnog žiga koristi se reverzibilno umetanje vodenog žiga. Temeljem toga postoje dvije glavne domene gdje se vodeni žig koristi:

- prostorna – implementacija na hardveru jer pruža manju računalnu složenost u usporedbi s frekvencijskom. Najjednostavniji takav primjer je algoritam temeljen na širenju razlike
- frekvencijska

Enkoder i dekoder dva su glavna dijela reverzibilnog sustava pri čemu su ugrađeni bitovi ili podaci o vodenom žigu umetnuti u sliku kroz proces enkodiranja. Proces dekodiranja koristi se za određivanje podataka o vodenom žigu prisutnih u slici, kao i njihovo izdvajanje do povrata u izvornu sliku. [45]

Algoritam temeljen na širenju razlike (eng. *difference expansion-based algorithm, DE*)

Prvi koji je predstavio ovaj algoritam bio je Tian Juan. Algoritam se temelji na proširenju razlike dvaju susjednih piksela [46]. Na primjeru razmatramo sivu sliku veličine 4x4 piksela s 8-bitnom dubinom koja ima ukupno 16 različitih intenziteta sive, kako je prikazano jednadžbom:

$$f(x,y) = \begin{bmatrix} 183 & 132 & 171 & 168 \\ 109 & 65 & 126 & 156 \\ 72 & 46 & 114 & 136 \\ 79 & 78 & 133 & 116 \end{bmatrix}$$

Uzimanjem 2 susjedna piksela postoji ukupno 8 slučajeva što se formira kao:

1. slučaj: [183, 132]
2. slučaj: [171, 168]
3. slučaj: [109, 65] itd.

Prema Tianu, za prvi slučaj razlika (D, eng. *difference*):

$$D = x - y = 183 - 132 = 51$$

gdje se prosjek tih piksela računa pomoću:

$$l = \left\lfloor \frac{x + y}{2} \right\rfloor = \left\lfloor \frac{183 + 132}{2} \right\rfloor = 157$$

Novo-proširena razlika izračunava se dodavanjem jednog ugrađenog bita nakon najmanje značajnog bita (*LSB,* eng. *least significant bit*).

$$D = (51)_{10} = (110011)_2$$

Neka je ugrađeni bit (b) jednak 1, a nova proširena razlika D':

$$D' = (110011b)_2 = (1100111)_2 = (103)_{10}$$

Slijedi izračun odgovarajućih vrijednosti slike sa vodenim žigom za piksele u prvom slučaju:

$$\mathrm{x}' = l + \left\lfloor \frac{\mathrm{D}' + 1}{2} \right\rfloor = 157 + \left\lfloor \frac{103 + 1}{2} \right\rfloor = 157 + 52 = 209$$

$$y' = l - \left\lfloor \frac{D}{2} \right\rfloor = 157 - \left\lfloor \frac{103}{2} \right\rfloor = 157 - 51 = 106$$

Na sličan način, izračunavaju se vrijednosti piksela s vodenim žigom za preostale slučajeve. Pružen je uvjet kako bi se prevladali problemi „podljeva“ (eng. *underflow*) i „odlijeva“ (eng. *overflow*). Uvjeti granice postavljaju se kao:

$$0 \leq l + \left\lfloor \frac{D + 1}{2} \right\rfloor \leq 255$$

$$0 \leq l - \left\lfloor \frac{D}{2} \right\rfloor \leq 255$$

Što znači da prethodne jednadžbe možemo zapisati kao:

$$|D| \leq 2(255 - l) \quad ako \quad 128 \leq l \leq 255$$

$$|D| \leq 2(l + 1) \quad ako \quad 0 \leq l \leq 127$$

Oblik slike s vodenim žigom stoga možemo zapisati kao: $w(x, y)$, tj.

$$w(x, y) = \begin{bmatrix} 209 & 106 & 173 & 166 \\ 132 & 43 & 172 & 111 \\ 86 & 33 & 148 & 103 \\ 80 & 77 & 142 & 107 \end{bmatrix}$$

Proces dekodiranja

Slično kao u procesu enkodiranja, razmatra se osam slučajeva uzimanjem dva susjedna piksela iz slike s vodenim žigom, a zatim se računaju prosjek (l'):

$$l' = \left\lfloor \frac{x' + y'}{2} \right\rfloor = \left\lfloor \frac{209 + 126}{2} \right\rfloor = 157$$

i razlika (D'):

$$D' = x' - y' = 209 - 106 = 103 = (1100111)_2$$

Stvarna razlika D pronalazi se izvlačenjem najmanje značajnog bita iz D':

$$D = (110011)_2 = (51)_{10}$$

Originalna izvorna slika (eng. *cover image*) za prvi se slučaj računa cjelobrojnom inverznom transformacijom:

$$x' = l' + \left\lfloor \frac{D + 1}{2} \right\rfloor = 157 + \left\lfloor \frac{51 + 1}{2} \right\rfloor = 157 + 26 = 183$$

$$y' = l' - \left\lfloor \frac{D}{2} \right\rfloor = 157 - \left\lfloor \frac{51}{2} \right\rfloor = 157 - 25 = 132$$

Da bismo dobili dekodiranu sliku, potrebno je na isti način izračunati preostale slučajeve. Nakon utvrđivanja vrijednosti intenziteta sive dekodirane slike i potpunog preklapanja sa vrijednostima izvorne slike, potvrđena je reverzibilnost – povrat slike bez gubitka informacija.

5.4. Biometrijska privatnost ili biometrija (eng. *biometrics*)

Definicija 4. *Biometrijski sustav je u osnovi automatizirani sustav za prepoznavanje uzoraka koji vrše identifikaciju ili verifikaciju identiteta utvrđivanjem vjerojatnosti da je određena fiziološka ili bihevioralna (npr. otisak prsta, prepoznavanje lica, zjenice, glasa i sl.) karakteristika valjana.*

Korištena metoda odmah je objedinjena definicijom polazišnog pojma, točnije provodi se skeniranjem, snimanjem i analizom spomenutih anatomskih karakteristika. Povezano s tim, ključevi predstavljaju jedinstvenost upravo tih karakteristika koje se koriste pri identifikaciji i verifikaciji o čemu će biti riječ niže.

Proces enkripcije: pretvorba biometrijskih podataka (npr. sken lica) pretvara se u šifrirani format prije pohrane i slanja mrežom

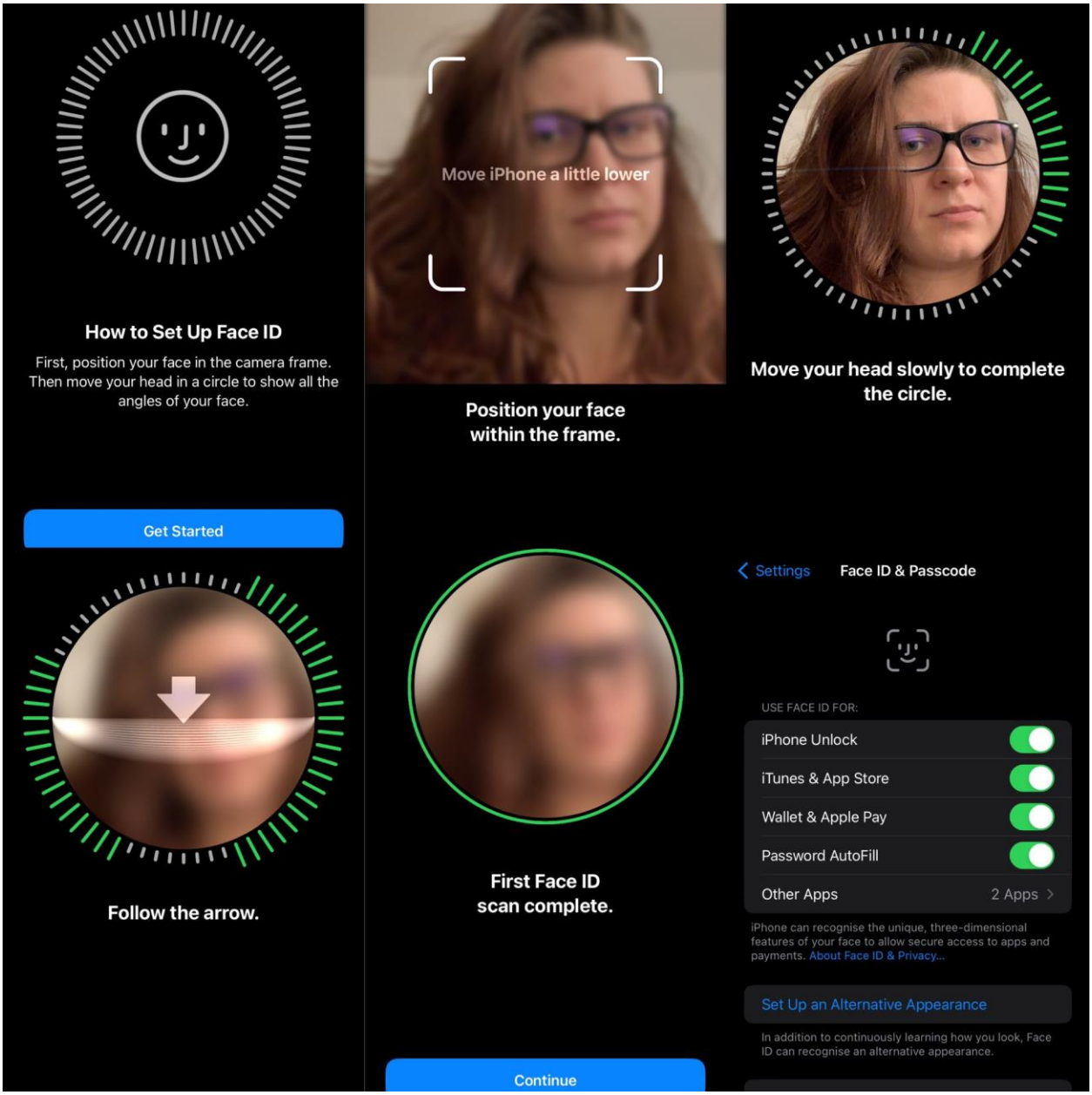
Proces dekripcije: ovjeravanje biometrijskih podataka, otkrivanje identiteta osobe te omogućavanje pristupa određenim resursima

Dok konvencionalna sredstva poput lozinki imaju problem u smislu krađe, gubitka i oslanjanja na pamćenje/memoriju korisnika, biometrijsku autentifikaciju moguće je postići kroz 2 prethodno najavljene metode:

1. metoda **verifikacije** – brz odgovor jer se podudaranje izvodi samo jednom iako korisnik mora unijeti svoj identitet za svaku sesiju provjere
2. metoda **identifikacije** – korisnik ne daje tvrdnju o identitetu, ali prepoznavanje jednog upita zahtijeva pretraživanje cijele baze podataka biometrijskih slika što rezultira dužim vremenom „odaziva“ (eng. *response time*) [47]

Budući da su biometrijski predlošci obično pohranjeni u obliku slika upita (eng. *query image*), vizualna se kriptografija koristi u kombinaciji s tehnikom steganografije. Biometrijske informacije, poput privatnih slika lica se šalju pouzdanom entitetu treće strane koji ih dekomponiraju na dva dijela i zatim pohrane u odvojene baze podataka. Dekomponirana slika ili dijelovi ne otkrivaju nikakve informacije o originalnoj slici. Time je osigurano da se privatna slika može otkriti samo kada su oba dijela istovremeno dostupna, a identitet nije otkriven niti jednom poslužitelju. [48]

Najpoznatiji takav primjer vidljiv je i na slici 40 koja detaljno prikazuje postupak postavljanja Face ID[16]-a, odnosno snimanja glave za potrebe zaključavanja uređaja i limitiranja pristupa pojedinim aplikacijama.

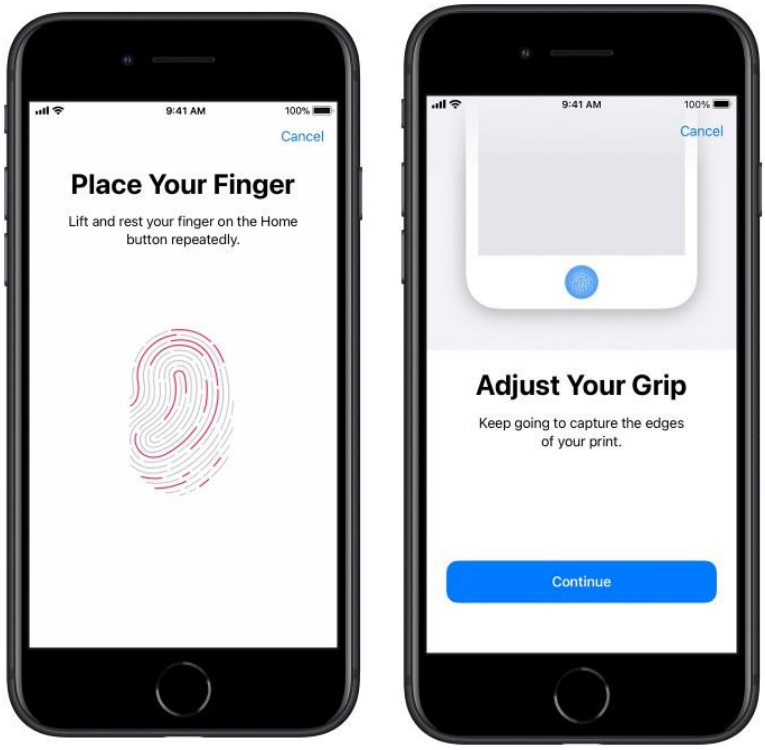


Slika 40. Postavljanje Face ID-a na osobnom uređaju, iPhone XR (iOS 16.5)

[16] Uređaj u osobnom, autorskom vlasništvu i postavljanje fotografija na vlastitu odgovornost

Za proces autentifikacije, svaki pojedinačni dio preklopljen je drugom slikom koja se bira iz javne baze.

Biometrija igra glavnu ulogu u današnjim sigurnosnim aplikacijama (npr. m-bankarstvo), uključujući i komercijalne svrhe poput e-trgovine te različitim oblicima kontrole pristupa (bankomati ili prijava na računalo). Različite vrste biometrije kao što su šarenica oka, prepoznavanje lica, otisci prstiju [49] (vidljivo na slici 41 [50]) i sl. koriste se za aplikacije za identifikaciju i provjeru identiteta.



Slika 41. Postavljanje Touch ID-a na iPhoneu SE (iOS 15)

Ukratko, spoj vizualne kriptografije, digitalnog sadržaja i biometrije leži upravo u primjerima autentifikacije koja je potrebna pri autorizaciji skrivenih ili privatnih podataka.

5.5. *Gaming*

Definicija 5. *Gaming ili na hrvatskom, igranje video igara, predstavlja oblik zabave koji uključuje interaktivno sudjelovanje korisnika, tj. drugih igrača (eng. gamers) putem video igara na različitim platformama kao što su računala (stolna ili prijenosna), igraće konzole i mobilni uređaji. Spomenuta aktivnost može se odvijati samostalno ili u društvu, uključujući i online interakciju s drugim igračima putem interneta. S druge strane, video igra elektronička je igra koja se pokreće joystickom, mišem, tipkovnicom ili kombinacijom navedenih ulaznih uređaja, a sve u svrhu manipulacije pokretnih figura na zaslonu.*

Obzirom na dosta generaliziranu definiciju, za razliku od ostalih primjera primjene vizualne kriptografije, *gaming* može biti opisan kroz sve 3 kategorije razmatranja:

1. kod – izbor popularnih programskih jezika koji se koriste u razvoju videoigara (igračka logika i mrežni kod); npr. C++ za *Counter Strike: Global Offensive*
2. kriptosustav – upotreba kriptografskih protokola SSL/TLS koja osigurava sigurnu komunikaciju između igraćeg računala i poslužitelja igre (npr. *World of Warcraft*)
3. potpisna shema (eng. *signature scheme*) – HMAC (*Hash-based Message Authentication Code*) kao algoritam koji se koristi za provjeru autentičnosti podataka (npr. online multiplayer igre poput *League of Legends, Call of Duty*, MMORPG-ovi poput *Final Fantasyja* i e-casisno za zaštitu financijskih transakcija
    a. javni (pohrana na server igre) i privatni (pripada igraču i koristi se za generiranje digitalnog potpisa) ključevi

Uz sve navedeno, u kontekstu igranja video igara, vizualna kriptografija može se iskoristiti za poboljšanje sigurnosti podataka i tehnike skrivanja. S povećanjem računalno-generirane grafike u igricama, zaštita osjetljivih informacija, kao što su: igrački resursi (eng. *assets*), podaci igrača i komunikacijski kanali, postaje ključna. Vizualna kriptografija pruža način za šifriranje i dijeljenje vizualnih informacija među različitim subjektima uključenim u *gaming* ekosustav, osiguravajući da se izvorni sadržaj sačuva.

Potencijalna primjena u *gaming*-u je sprječavanje situacija s varanjem (eng. *cheating scenarios*). Jedan od takvih primjera je i Ricocheat koji se spominje u kontekstu igrice *Call of Duty*, a opisan je kao mehanika koja preusmjerava štetu na igrača koji ju je izazvao.

Koristi se kod namjernog uništavanja suigrača ili ponašanja koje ometa tim, a djeluje po principu da ako igrač pogodi ili ubije vlastitog suigrača šteta mu se reflektira i završava s pogubnim, po njega samog, posljedicama.

S kriptografske strane, sheme vizualnog tajnog dijeljenja (eng. *CPVSS schemes; cheating-prevention visual secret-sharing*) mogu se koristiti za identifikaciju varalica (eng. *cheaters*) u igricama za više igrača (eng. *multiplayer games*). Ukratko, varalice su zlonamjerni sudionici koji imaju namjeru saznati tajnu, a u kontekstu vizualne kriptografije sposobni su čak i kreirati lažne udjele (eng. *fake shares*). Cijeli proces može lako „suspendirati" sumnjivca ukoliko se na početku svim pouzdanim sudionicima dodijeli i verifikacijska slika. Postoje dvije vrste varalica MP (eng. *malicious participant*), odnosno ZS (zlonamjerni sudionik) i MO (eng. *malicious outsider*), odnosno ZA (zlonamjerni autsajder). [51] Faze varanja su:

1. konstrukcija lažnih udjela (eng. *fake shares construction*) – varalica kreira lažne udjele
2. rekonstrukcija slike – pojava lažne slike nastale preklapanjem lažnih udjela s originalnim

Cijeli proces varanja smatra se uspješnim ukoliko iskreni sudionici koji pokažu svoje udjele za rekonstrukciju tajne slike nisu sposobni prepoznati lažne udjele od originalnih. Rekonstrukcija kao takva u potpunosti se oslanja na svojstvo savršene crnoće (eng. *perfect blackness property*) koje kaže da je slika rekonstruirana savršeno ako je svaki subpiksel koji je povezan s crnim pikselom tajne slike isto crn. Posljednje prije konkretnih primjera ostaje objasniti tri metode varanja:

- varanje od strane zlonamjernog sudionika – može biti među kvalificiranim sudionicima (eng. *qualified participants*). Zlonamjerni sudionik koristi originalni udio za kreiranje lažnog koji nije primjetno i vizualno drugačiji, dok je output slika drugačija od originalne tajne.
- varanje od strane zlonamjernog autsajdera (ZA) – diskvalificirani sudionik koristi nasumične slike za kreiranje lažne. Dodatno, kreira lažne udjele različitih veličina što se kasnije odražava i na veličini udjela originala.

- varanje u proširenoj vizualnoj kriptografiji – ZS stvara lažni udio iz legitimnog razmjenjujući crne piksele sa bijelim što dovodi do manjeg kontrasta rekonstruirane slike. Što je kontrast manji, teže se vidi slika unutar rekonstruirane. Lažna slika u naslagivanju lažnih udjela ima dovoljno kontrasta u odnosu na pozadinu te se čak i u prisutnosti savršene crnoće može obnoviti.

U kontekstu slika u *gaming*-u, primjena povjerljivih shema usmjerava se na sprječavanje manipulacije ili kršenja pravila [52] uz vizualne elemente:

1. sustav protiv detekcije i sprječavanja hakiranja tekstura (npr. *wallhack*) – omogućava igračima da vide protivnike kroz zidove; primjer igrice CSGO kao što je vidljivo na slici 42

Slika 42. Wallhack u igrici CSGO

Kako bi *wallhack* bio funkcionalan potrebno je kupiti konfiguracijske datoteke, skripte ili softvera koji modificiraju igru, a do njih se dolazi preko online preprodavača. Kupovinom spomenutog, mijenja se ponašanje memorije i grafike, dok igrač zauzvrat dobiva mogućnosti:

- uklanjanja ili promjene teksture zidova
- dodavanja ili mijenjanja boja i obrisa igrača čineći ih vidljivim, svjetlijim ili sjajnijim (isticanje na bilo koji uočljiv način)
- prikazivanje informacija igrača kao što su: ime, zdravlje ili udaljenost [53]

2. zaštita autorskih prava – gdje postoji zakonodavni deficit, čini se da je iskazan suficit (povećanje) piratstva, čak i u igrama, barem gdje to dopuštaju developeri stoga se zahtijeva donošenje zakonodavnih akata koji se odnose na zaštitu digitalnog sadržaja [54]
3. vizualna identifikacija – primjenjivo za igre s elementima kao što je avatar ili korisnički profil kako bi se osiguralo da je korisnik zaista osoba koja i kakvom se predstavlja sprječavajući korištenje lažnih ili neovlaštenih profila. Prvi primjer koju je zaokupio pažnju Rediti [55] bila bi igrica *Lost Ark*, sa slike 43, koja je uvela CAPTCHA sustav sa 3 pokušaja. Ukoliko bi igrač dao 3 pogrešna unosa dobiva trajno izbacivanje (eng. permanent ban)

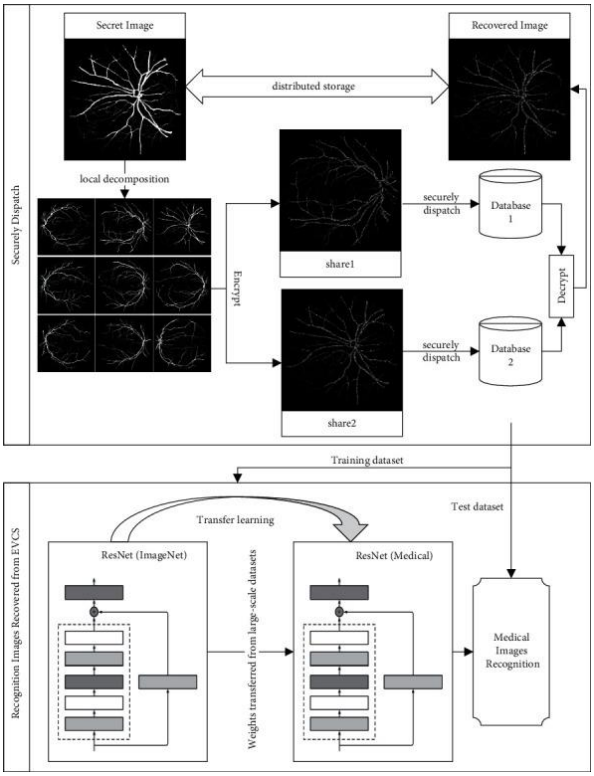
Slika 43. CAPTCHA sustav u Lost Ark igri

Iako se digitalni sadržaj i dalje može ilegalno kopirati, objaviti ili distribuirati na neki treći način, korištenje spomenutih primjera pomaže u stvaranju poštenog i uravnoteženog igraćeg okruženja. Pojedini igrači mogu biti i nagrađeni za pošteno sudjelovanje (eng. *fair play*) čime se u konačnici održava integritet *gaming* okruženja.

6. Budućnost i očekivani trendovi upotrebe

I(K)T nije jedina branša koja može profitirati napredovanjem vizualne kriptografije. Tu su i trendovi poput:

- zdravstva – prijenos biomedicinskih podataka, kao dio IoMT-a (eng. *Internet of Medical Things*), kroz otvorenu i nepouzdanu mrežu predstavlja novi izazov za zaštitu podataka o pacijentima. Sigurnosni problemi s tehnologijom koja pohranjuje, šalje i prima medicinske podatke mogu dovesti do izlaganja osobnih zdravstvenih informacija online. Osobne medicinske slike, npr. MRI ili CT, trebaju biti povjerljive kako bi se izbjegao problem ugrožene privatnosti pacijenta. Teoretski, moderna kriptografija s javnim ključem i vodenim žigom bi se mogla koristiti, ali zbog ograničenja slikovnih podataka i prikupljanja podataka u stvarnom vremenu, potrebne su brže i jednostavnije metode. Model prikazan na slici 44 temelji se na shemi vizualne kriptografije bez proširenja piksela. Isprva, osjetljivu sliku dijelimo na nekoliko nepovezanih slika te ih neovisno prenosimo i pohranjujemo kako bismo osigurali siguran prijenos. Kako bismo riješili problem da šum dešifrirane slike ometa izvedbu prepoznavanja, dobivamo „težine prije treninga“ (eng. *pretraining weights*) iz velikih skupova podataka (eng. *large-scale datasets*) i prenosim ih na vizualno-kriptografski bazirane mreže za prepoznavanje skupova podataka s gubitkom (eng. *lossy dataset recognition*) putem metode prijenosnog učenja (eng. *transfer learning*. Ovakve i puno detaljnije kriptografske sheme



Slika 44. Visoko-precizna mreža za prepoznavanje medicinskih slika (bazirana na vizualnoj kriptografiji)

[56] potrebne su u svrhu ostvarenja učinkovite implementacije i sofisticirane komunikacije.

- komunikacije – napredak se nastoji očitovati kroz sigurniju razmjenu informacija što uključuje poboljšanja u aplikacijama koje podržavaju razmjenu:
    - poruka – poput WhatsApp-a [57] i *end-to-end* enkripcije u kojoj samo krajnji primatelj može dešifrirati (pročitati) poruke čime je nemoguće prisluškivati (eng. *eavesdropping*)
    - video sadržaja – općenito se to odnosi na protokole (TLS/SSL) koji osiguravaju sigurnosni prijenos, dok se od krajnjeg korisnika traži bilo kakav oblik autentifikacije (npr. *Zoom* svojim korisnicima omogućava 2FA [58] ili potpuna preklapanja u pristupnim podacima, konkretnije, ukoliko korisnik nije registriran na zadanu domenu [59] – nema priključivanja na sastanak ili *webinar*)
- marketinga – pri čemu se misli na kampanje i promocije novo-plasiranog proizvoda na tržište. Ovako se nov pojam odmah približava potencijalnoj publici i od njih zahtijeva stupanje u interakciju. Jedan od poznatijih primjera je McDonald's-ov „*Shamrock Shake*" koji je 2017. lansirao promociju koja uključuje tajnu poruku skrivenu unutar grafike na plakatu. Svi korisnici koji su uspješno dešifrirali zadano su ujedno i otkrili tajno mjesto zabave za dan svetog Patrika.

Uz upravljanje digitalnim pravima i pripadajuće dostupnim tehnologijama, sve više poslovanja prisvojit će najbolje prakse digitalnih medija i njihove pohrane u DAM (*Digital Asset Management*) što će pozitivno utjecati na strateški razvoj organizacije/poduzeća. Prednosti su vidljive kroz:

- cjenovnu pristupačnost – troškovi pohrane su optimizirani jer je sve na jednom, centralnom, mjestu [60]
- učinkovitost upravljanja resursima – efikasna organizacija, kategorizacija (katalogizacija i indeksiranje sadržaja) te brža pretraga digitalnih resursa kako od strane čovjeka, tako od strane tražilica na računalu
- povećana suradnja i komunikacija – dijeljenje digitalnih medija unutar timova i organizacije; naglasak na lakom pristupu i ažuriranju zajedničkih resursa

- bolja kontrola pristupa i sigurnost – osiguranje da samo ovlaštene osobe pristupaju određenim digitalnim resursima

Kako stvari stoje, DAM u poveznici sa prodajnim API-jem (eng. *Application Programming Interface*), kroz radni tijek (eng. *workflow*) donosi dvije struje budućnosti:

1. mikro – izgradnja malog sustava koji se može prodati različitim poduzećima gdje proizvođač/prodavač naplaćuje prilagodbu, a kupac kupuje i druge proizvode iz linije kako bi postigao ciljeve optimiziranog upravljanja digitalnim sredstvima
2. makro – tvrtke koje kupuju prava na sve dijelove digitalnog lanca čime bježe iz najma i dugoročnog obvezivanja što se čini gotovo nemogućim. Modelom vlasništva umjesto pristupa najbliže je došao Microsoftov SharePoint koji prednjači po brojnim pogodnostima. [61]

Ostaje za vidjeti, kada će i koja mega-korporacija ponuditi odgovor na potpuno integriranu platformu za upravljanje digitalnim sredstvima, a da je pritom digitalno inkluzivna i pouzdana sa sigurnosnog aspekta.

7. Zaključak

Evidentno je da se iskazuje hitna potreba za promišljanjem tradicionalnih zapisa i prava te redefiniciji imovine i njenoj ekstenziji na virtualne/digitalne objekte. Neki budući, novo-doneseni zakon, uz smanjenje troškova, trebao bi regulirati odnose od pružatelja usluga preko rizika koji se povezuju s njima sve do krajnjeg korisnika, samog klijenta. Isti mora biti sveobuhvatan [62] i neisključiv jer se samo tako može osigurati stabilnost i uzajamno povjerenje.

Imajući na umu sve navedeno, važno je naglasiti i činjenicu da upravljanje digitalnim sadržajem i imovinom uključuje brojne faktore od kojih svaki mora biti u skladu s važećim propisima. Primjer bi bio i ovaj cjelokupni diplomski rad koji koristi sadržaj poput teksta, slika, informativnih grafika i sl. Svaki dio koji nije samostalno osmišljen ima vrijednost daleko veću od cijene same izrade. Samim time, ispitujući autorska prava, imenovanjem autora koji su doprinijeli poboljšanju rada te pravilnim citiranjem i navođenjem izvora smanjuje se rizik od potencijalnih prigovora ili tužbi. Srećom, vlasnici prava i distributeri sada imaju korist od brojnih tehnologija koje su osmišljene u svrhu dodatnog očuvanja i zaštite vrijednosti imovine. Dobar dio istih svodi se na neke od prethodno spomenutih principa vizualne kriptografije kao što su vodeni žigovi ili DRM (eng. *Digital Management Rights*). Zajedno, svi alati imaju širok raspon i nastoje osigurati sadržaj utoliko da je on dostupan sam legitimnim korisnicima.

A kako znati je li netko uistinu legitiman korisnik, pogotovo u vrijeme kad je sve dostupno na dlanu i jednim klikom, Bruce Schneier, američki kriptograf i stručnjak za računalnu sigurnost, pojasnio je kroz izjavu: *„Nijedan sustav kriptiranja nije neprobojan. Ali, kriptografija je kao zatvor. Onaj tko pokuša pobjeći, radi to na svoj vlastiti rizik.“* Te riječi potvrđuju i mnogi zviždači za koje se povlače polemike jesu li zapravo moderni heroji, izdajice ili hrabriji od većine; samo što je upitno, kao i svi dostupni podaci, „*koliko je to zapravo **vrijedno**?*“.

8. Popis literature

[1] A. Dujella i M. Maretić, Kriptografija, Zagreb: Element, 2007.

[2] K.-H. Jung i R. Srinivasan, »ResearchGate: Cryptographic and Information Security Approaches for Images and Videos,« Siječanj 2019.. [Mrežno]. Available: https://www.researchgate.net/publication/330440535_Cryptographic_and_Information_Security_Approaches_for_Images_and_Videos. [Pokušaj pristupa 10 Travanj 2023.].

[3] M. Naor i A. Shamir, »Visual Cryptography,« u *Advances in Cryptology—EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques*, Rehovot, 1994..

[4] S. Pavlovsky, »Youtube,« Liquid Light Lab, 15 Studeni 2019.. [Mrežno]. Available: https://youtu.be/vn7_ctQjqhE. [Pokušaj pristupa 3 Lipanj 2023.].

[5] D. Schmolze, C. Standley, K. Fogarty i A. Fischer, »ResearchGate; Advances in Microscopy Techniques,« Veljača 2011. [Mrežno]. Available: https://www.researchgate.net/publication/49801393_Advances_in_Microscopy_Techniques. [Pokušaj pristupa 3 Lipanj 2023].

[6] D. Jena i S. K. Jena, »IEEE Xplore,« 2009.. [Mrežno]. Available: https://ieeexplore.ieee.org/abstract/document/4777337. [Pokušaj pristupa 3 Lipanj 2023.].

[7] K. Linda, »WIRED,« 31 Siječanj 2019. [Mrežno]. Available: https://www.wired.com/story/finding-lena-the-patron-saint-of-jpegs/.

[8] »Fakultet informatike u Puli,« [Mrežno]. Available: https://fipu.unipu.hr/. [Pokušaj pristupa 14 Travanj 2023].

[9] Y.-H. Chen i J. S.-T. Juan, »XOR-Based (n, n) Visual Cryptography Schemes for Grayscale or Color Images with Meaningful Shares,« Applied Sciences 12, no. 19: 10096, 2022.

[10] D. Shaked, N. Arad, A. Fitzhugh i I. Sobel, »HP Tech Reports,« svibanj 1999. [Mrežno]. Available: https://www.hpl.hp.com/techreports/96/HPL-96-128R1.pdf.

[11] Y.-C. Hou, »Patter Recognition, Volume 36, Issue 7,« u *Visual cryptography for color images*, 2003, pp. 1619-1629.

[12] X. Wu i W. Sun, »Extended Capabilities for XOR-Based Visual Cryptography,« IEEE Transactions on Information Forensics and Security, N/A; online, 2014.

[13] Z. Wang, Z. Xu i X. Jia, »SXVCS: An XOR-based Visual Cryptography Scheme without Noise via Linear Algebra,« Cornell University; arXiv, 2022.

[14] Y.-H. Chen i J. S.-T. Juan, »XOR-Based (n, n) Visual Cryptography Schemes for Grayscale or Color Images with Meaningful Shares,« MDPI, Puli, Nantou, 2022.

[15] R. Al-Khalid, R. A. Al-Dallah, A. Al-Anani, R. M. Barham i S. Hajir, »A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes,« SCRIP, Al-Balqa i Amman, Jordan, 2017.

[16] NASA, »Science NASA,« [Mrežno]. Available: https://science.nasa.gov/ems/09_visiblelight/.

[17] V. Rebić, »hrcak.srce.hr,« 2008. [Mrežno]. Available: https://hrcak.srce.hr/file/121262.

[18] Y.-C. Hou, »Visual cryptography for color images,« ELSEVIER, 2003.

[19] A. A. Stonier, K. Praghash i V. Ganji, »CMY Color Spaced-Based Visual Cryptography Scheme for Secret Sharing of Data,« Hindawi, London, 2022.

[20] A. MaungMaung i H. Kiya, »StyleGAN Encoder-Based Attack for Block Scrambled Face Images,« Cornell University, arXiv, Ithaca, 2022.

[21] E. L. i Brian, »Error Diffusion Halftoning Methods for Image Display,« The University of Texas at Austin, Austin, 2008.

[22] K. Venugopal, Rishvanth, R. J. Heath i D. L. Lau, »FPGA Based Parallel Architecture Implementation of Blue-Noise Multitoning with Stacked,« Department of Electrical and Computer Engineering, University of Kentucky, Lexington, 2013.

[23] S. Pigeon, »Harder, Better, Faster, Stronger Explorations in better, faster, stronger code.,« 31 Prosinac 2013. [Mrežno]. Available: https://hbfs.wordpress.com/2013/12/31/dithering/.

[24] T. Helland, »tannerhelland.com,« 28 Prosinac 2012. [Mrežno]. Available: https://tannerhelland.com/2012/12/28/dithering-eleven-algorithms-source-code.html.

[25] christian, »Scipython,« 13 Listopad 2021. [Mrežno]. Available: https://scipython.com/blog/floyd-steinberg-dithering/.

[26] D. Shaked, N. Arad, A. Fitzhugh i I. Sobel, »Color Diffusion: Error-Diffusion,« HP Laboratories Israel, 1999..

[27] K. Bhat, U. K. K.R. Reddy, R. H.S. Kumar i D. Mahto, »A novel scheme for lossless authenticated multiple secret images sharing using polynomials and extended visual cryptography,« IET; The Institution of Engineering and Technology, Stevenage, 2020.

[28] A. Hakeem, S. A. i H. Kim, »Centralized Threshold Key Generation Protocol Based on Shamir Secret Sharing and HMAC Authentication,« mdpi, 2022.

[29] D. Somwanshi i V. T. Humbe, »A Secure and Verifiable Color Visual Cryptography Scheme with LSB Based Image Steganography,« WARSE, Maharashtra, 2021.

[30] J.-Y. Lin i J. S.-T. Juan, »Fault-Tolerant Visual 2-Secrets Sharing Scheme,« WSCE, Beijing, 2017.

[31] Y. A. Hamza, N. E. Tewfiq i M. Q. Ahmed, »An Enhanced Approach of Image Steganographic Using Discrete Shearlet Transform and Secret Sharing,« Baghdad Science Journal, Duhok i Mosul, Irak,

2022.

[32] L. Ren i Z. Denghui, »A QR code-based user-friendly visual cryptography scheme,« 2022. [Mrežno]. Available: https://www.nature.com/articles/s41598-022-11871-9.pdf.

[33] K. R. Vineetha i K. Sinu, »Design And Implementation of Secure Qr Payment,« International Journal for Multidisciplinary Research (IJFMR), Nehru, 2023.

[34] M. Li, F. Yin, L. Song, X. Mao, F. Li i C. Fan, »Nucleic Acid Tests for Clinical Translation,« American Chemical Society, 2021.

[35] A. Arora, H. Garg i S. Shivani, »Privacy Protection of Digital Images Using Watermarking and QR,« Hindawi, Mathura i Punjab, Indija, 2023.

[36] Y.-W. Chow, W. Susilo, J. Tonien, Vlahu-Gjorgievska i G. Yang, »Cooperative Secret Sharing Using QR Codes and Symmetric Keys,« School of Computing and Information Technology, Wollongong, 2018..

[37] K. Patil S., S. Bhagate B. i D. M. Kuklarni, »Overview of Visual Secret Sharing Schemes for QR,« Department of Computer Science, D.K.T.E. Society's Textile and Engineering Institute, Ichalkaranji, 2018..

[38] X. Cao, L. Feng, P. Cao i J. Hu, »Secure QR Code Scheme Based on Visual Cryptography,« u *2016 2nd International Conference on Artificial Intelligence and Industrial Engineering (AIIE 2016)*, 2016.

[39] »OSIBeyond,« 14 srpanj 2022.. [Mrežno]. Available: https://www.osibeyond.com/blog/single-factor-authentication-is-now-officially-a-bad-practice/.

[40] B. Rezanov i H. Kuchuk, »Advanced Information Systems, Vol. 6, No. 2,« 2022. [Mrežno]. Available: http://ais.khpi.edu.ua/article/view/260681/257093.

[41] D. Glusezim, Z. Seiitkaliyeva, A. Razaque i A. Oun, »Two Factor Authentication using Twofish Encryption and Visual Cryptography Algorithms for Secure Data Communication,« u *Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 2019.

[42] N. Abapour i M. Ebadpour, »Cronell University - arXiv,« 2022. [Mrežno]. Available: https://arxiv.org/pdf/2204.08017.pdf.

[43] R. J. Hwang, »Semantic Scholar,« Tamkang Journal of science and Engineering, 2000. [Mrežno]. Available: https://www.semanticscholar.org/paper/A-Digital-Image-Copyright-Protection-Scheme-Based-Hwang/537e845dda5f0db03c394632e3bd9e06eac173bc.

[44] A. Fatahbeygi i A. F. Tab, »A highly robust and secure image watermarking based on classification and visual cryptography,« u *Journal of Information Security and Applications (JISA)*, Guildford, ELSEVIER, 2019, pp. 71-78.

[45] Das, J. S. Subhajit i Arun, »A Study on Reversible Image Watermarking Using Xilinx System

Generator,« u *Computational Intelligence in Pattern Recognition*, Singapur, Springer, 2020, pp. 233-236.

[46] J. Tian, »IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 890-896,« kolovoz 2003. [Mrežno].

[47] S. M. Thampi, P. K. F. C.-I. Atrey i G. Perez Martinez, Security in Computing and Communications, London: Springer, 2013.

[48] A. Ross i A. Othman A, »ResearchGate,« Travanj 2011. [Mrežno]. Available: https://www.researchgate.net/publication/224202987_Visual_Cryptography_for_Biometric_Privacy. [Pokušaj pristupa 20 Lipanj 2023].

[49] B. Dorizzi, R. L. Haddada i N. Ben Amara Essoukri, »A combined watermarking approach for securing biometric data,« u *Signal Processing: Image Communication*, Martigny, ELSEVIER (Idiap Research Institute), 2017, pp. 23-31.

[50] anonimno, »Apple support,« Apple, 17 Ožujak 2022.. [Mrežno]. Available: https://support.apple.com/en-us/HT201371. [Pokušaj pristupa 20 Lipanj 2023.].

[51] P. Venny i J. Rao, »A Survey on Cheating Prevention with Verifiable Scheme,« International Journal of Computer Applications, Volume 133, No.16, Pune, 2016.

[52] I. Korzova, »ResearchGate,« Srpanj 2021. [Mrežno]. Available: https://www.researchgate.net/publication/357077782_Intellectual_Property_Issues_in_Video_Games.

[53] »iGaming.org,« [Mrežno]. Available: https://igaming.org/gaming/esports/wallhack/.

[54] B. S.B. i A. Tegza, »Protection of virtual gaming property: national and foreign experience,« Uzhhorod National University, Uzhhorod, 2022.

[55] L. (. k. ime), »Reddit,« 24 kolovoz 2022. [Mrežno]. Available: https://www.reddit.com/r/MMORPG/comments/wwmiwb/lost_ark_added_a_captcha_system_and_if_you_fail_3/.

[56] L. Ren i D. Zhang, »A New Data Model for the Privacy Protection of Medical Images,« u *Comput Intell Neurosci*, 2022.

[57] F. W. HelpCenter, »FAQ WhatsApp,« 2016. [Mrežno]. Available: https://faq.whatsapp.com/820124435853543.

[58] D. Z. aplikacije, »ZoomSupport,« 9 studeni 2023. [Mrežno]. Available: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0066054.

[59] Z. d. aplikacije, »ZoomSupport,« 21 studeni 2023. [Mrežno]. Available: https://support.zoom.com/hc/hr/article?id=zm_kb&sysparm_article=KB0061263.

[60] D. Austerberry, »Introduction to Digital Asset Management,« u *Digital Asset Management, Second Edition, Professional Video and Television File-based Libraries*, Oxford, Focal Press, 2006, pp. 10-21.

[61] E. Feguson Keathley, »DAM Is the Future of Work,« u *Digital Asset Management: Content Architectures, Project Management, and Creating Order Out of Media Chaos*, Apress, 2014, pp. 144-150.

[62] A. Kodynets i A. Murashko, »ResearchGate,« Rujan 2021. [Mrežno]. Available: https://www.researchgate.net/publication/354573601_Video_game_in_the_system_of_intellectual_property_the_concept_and_features_of_legal_protection.

[63] K. Dhiman i S. S. Kasana, »Extended visual cryptography techniques for true color images, Volume 70,« u *Computers & Electrical Engineering*, Elsevier, 2018, pp. 647-658.

[64] Y. Cachón Santana, »vixra.org,« 20 svibanj 2018. [Mrežno]. Available: https://vixra.org/pdf/1805.0352v1.pdf.

9. Popis slika

10. Sažetak i ključne riječi

Digitalizacija nudi brojne nove mogućnosti o kojima se nekada samo moglo sanjati, ali time je i otvorila vrata kršenju autorskih prava. Tematika zaštite digitalnog sadržaja time postaje ključ očuvanja kreativnosti i poticaja inovacija. Vizualna kriptografija, implementacijski naizgled jednostavna, doskočila je tome pomoć ponudom brojnih rješenja poput: dvofaktorske autentifikacije, biometrije, vodenih žigova pa čak i QR kodova koja se svakodnevno koriste, a da ljudi pritom nisu ni svjesni „pozadinskih procesa“. Samim time, pitanje zaštite više nije stvar samo kompleksnosti korištenih tehnologija pri implementaciji, već i bezbolne integracije u sustav uz minimalne troškove.

Ključne riječi: vizualna kriptografija, digitalni sadržaj, zaštita digitalnog sadržaja, autorska prava, digitalizacija

Abstract

Digitalization offers numerous new possibilities that were once only imaginable, but it has also opened the door to copyright infringement. The issue of protecting digital content has become crucial both for preserving creativity and fostering innovation. Visual cryptography, although seemingly straightforward in implementation, has tackled the challenge by offering numerous various solutions such as: two-factor authentication, biometrics, watermarks, and even QR codes. The mentioned are used daily without people even being aware of the underlying processes. As a result, the question of securing is no longer solely about the complexity of the technologies used in implementation, but also about seamless integration into the system with minimal costs.

Keywords: visual cryptography, digital content, securing digital content, copyright, digitalization