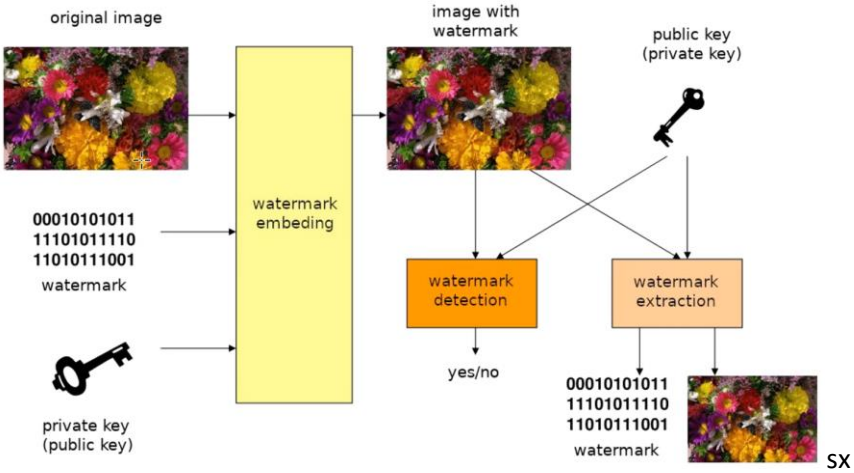
# Vodoznaky

- Motív vložený do obrázku viacej či menej viditeľným spôsobom aby bolo možné obrázok identifikovať po prípade ochrániť copyright
    - text, vzor...
- Je to nejaká informácia
- Vkladajú sa do obrázku tak aby ich nebolo vidieť
- Je vložený do obrázku tak, aby ho nebolo možné oddeliť



sx

## Klasifikácia

- Viditeľný/neviditeľný
- Metódy vkladania:
    - Priama zmena obrázku
    - Zmena frekvenčnej domény
    - . . .
- Typ dát:
    - Binárne data (neviditeľná metóda) – niekedy je vynucované plné zachovanie binárneho kódu, niekedy nie
    - Vloženie priamo obrázku, napr. Logo firmy… (viditelná metóda)
    - . . .

## Vlastnosti

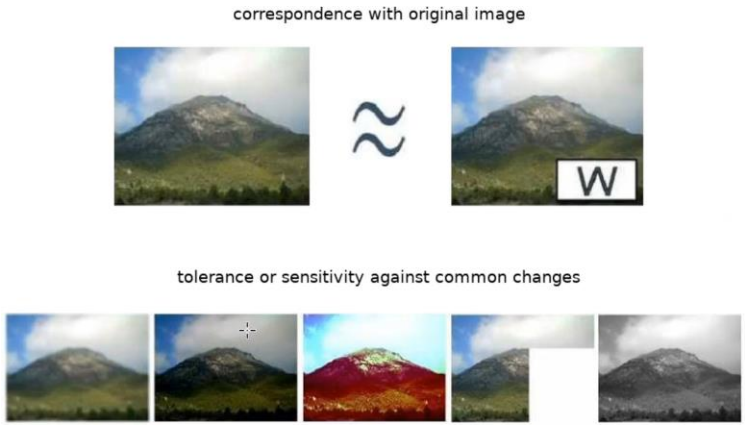
- Kapacita – koľko bitov sme schopný vložiť do obrázku vodoznaku, typicky stovky až tisíce
- Výpočetná zložitosť
- Granularita – veľkosť blokov v obrázku do ktorých sa vodoznaky vkladajú
- Viditeľnosť
- Rubostnosť/krechkosť – napr. pri ochrane vlastníctva, ak niekto ten obrázok upraví/oreže/otočí.. aby sa zachoval a bolo ho možné stale extrahovať
    - Krehký – zničí sa
    - Robustný – udrží sa
- Tolerancie – ako moc zmení obrázok, čo tolerujem
- Bezpečnosť – odolnosť vodoznaku, zložitosť odstránenia, pridania, dekódovania…

## Viditeľné vodoznaky

- Náročné odstránenie vodoznaku, ale spôsob existuje – neurónové siete, robustné analytické algoritmy… (ale stale je to poznať)

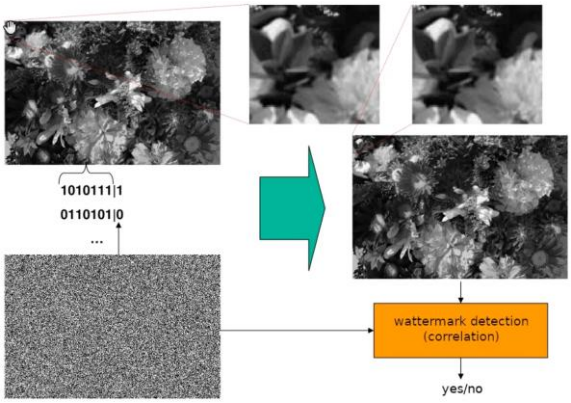

## Neviditeľné vodoznaky

- Užívateľ nie je schopný vôbec povedať, či sa v obrázku vodoznak nachádza – výhoda, keby o ňom vedel je schopný ho skôr odstrániť




## LSB modulácia

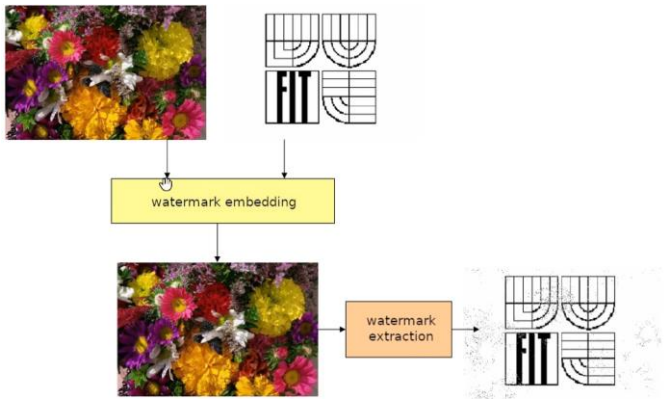
- Vodoznak je zakódovaný do najmenej významných bitov každého pixelu obrázku
- Nie je to robustná metóda, pretože akákoľvek manipúlácia s obrazom vodoznak zmaže – napr. pridanie šumu
- Robustné voči orezávaniu, či posúvaniu
- Môže to byť pseudonáhodná sekvencia
    - V prípade, že je tošum je možné využiť kľúč ktorý generuje ten šum
- Môže byť detekovaný pomocou kolerácie na úrovni signálu



- ***Pre RGB obrázky:***
    - Transformuje obrázok do jasovej bitmapy a tam zakódujem vodoznak, nie je ho možné nájsť v obrázku a je robustnejší voči zmenám farieb, ale za cenu strát vodoznaku, nedetekujem ho kompletne kvôli zanášaniu chyby výpočtom a zaokrúhlovaniu

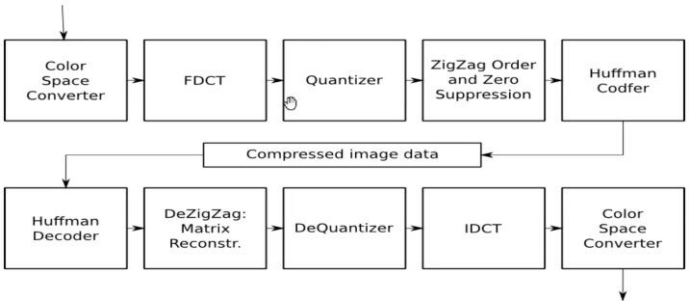
$$\begin{bmatrix} Y' \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.14713 & -0.28886 & 0.436 \\ 0.615 & -0.51499 & -0.10001 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1.13983 \\ 1 & -0.39465 & -0.58060 \\ 1 & 2.03211 & 0 \end{bmatrix} \begin{bmatrix} Y' \\ U \\ V \end{bmatrix}$$

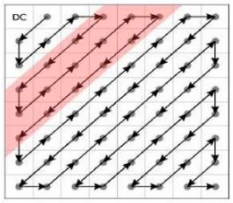


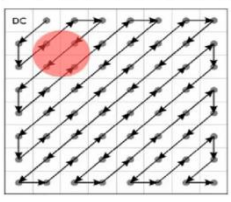

## Vkladanie vodoznaku použitím koeficientov dikrétnej kosínovej transformácií (DCT)

- LSB nie je robustné oproti stratovej kompresií JPEG alebo MPEG – vodoznak sa stratí počas kompresie
- Vodoznak sa vkladá vo fázi kvantizácie a ZigZag order and Zero Suppresion
- Vodoznak sa dekóduje vo fázy DeKvantizácie a IDCT

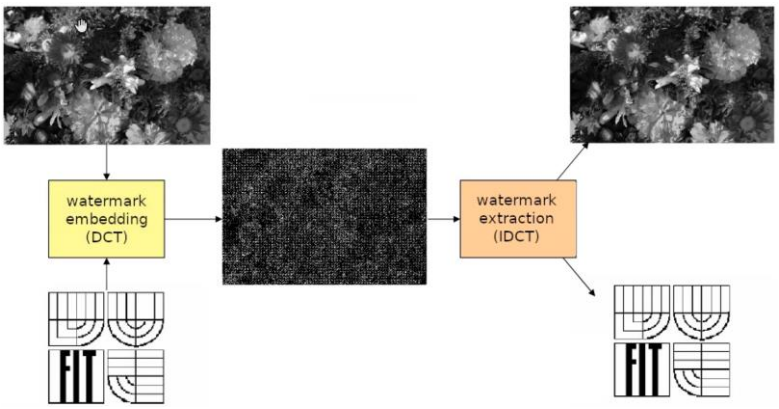



- Oveľa robustnejšia metóda a menej viditeľná vo výstupnom obraze
- Výsledok transformácie 8x8 pixelov vedie k 8x8 frekvenčných koeficientov
- Nemôže sa manipulať s koeficientmi podčerveným pásom, pretože kompresia nezaručí či vôbec sa budú nachádzať v obraze, a ani and pásom, pretože sú príliš dôležité a mohol by sa zmeniť výzor obrazu
- z červeného pásu sa vyberú nejaké štyry koeficienty, s ktorými sa bude manipulovať



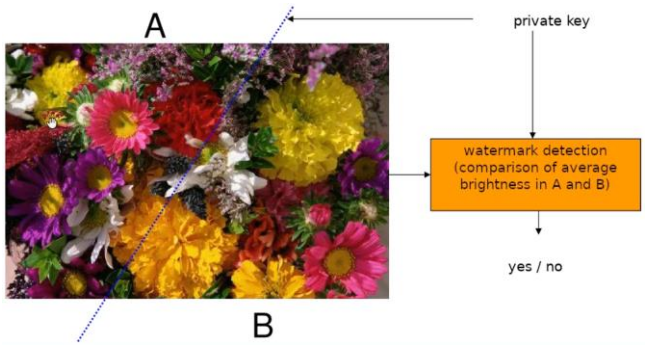

- nie je robustný voči orezávaniu




- touto metódou je možné vložiť vodoznak a očakávať pri extrákcií vodoznak bez chýb, bez zmien

## Disjoint sets

- obrázok reprezentovaný ako pole pixelov, z tohto pola vyberiem náhodne dve podmnožiny pixlov A a B vo forme zoznamu
- vybrané pixely sú súkromný kľúč
- intenzitu pixelov z množiny A zväčším o *k*
- intenzitu pixelov z množiny B zmenším o *k*
- zmeny musia byť radšej menšie aby boli neviditeľné na výstupnom obŕazku, po pŕipade z million pixlov vybrať len len dve podmnožiny napr. po 10 000 pixelov
- detekcia vodoznaku prebieha pomocou rozdelenia obrázku podľa súkromného kľúča
- spočítanie priemernej intensity
- ak sa tam nachádza vodoznak, tak rozdiel intenzít bude približne 2*k*, inak skoro 0

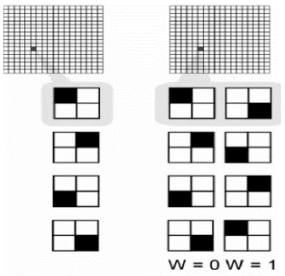



- nie je robustný voči orezávaniu, či posunu, ale odolný voči zmenám jasu a kontrastu

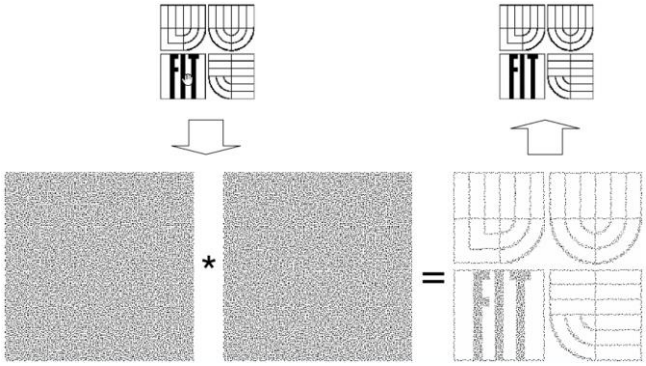
## Použitie MD5

- šifra MD5 je prelomená
- rozdelím obrázok na 8x8 pixelv
- zmažem LSB
- zbytok bytov je spojený s parametrom závislým na veľkosti obrázku a súkromného kľúča
- MD5 checksum je kombinovaný s binárnym obrázkom vodoznaku
- Výsledok je vložený do obrázku ako LSB
- Krehký ale dobre detekovateľn ý a nezistiteľný

## Vizuálna kryptografia

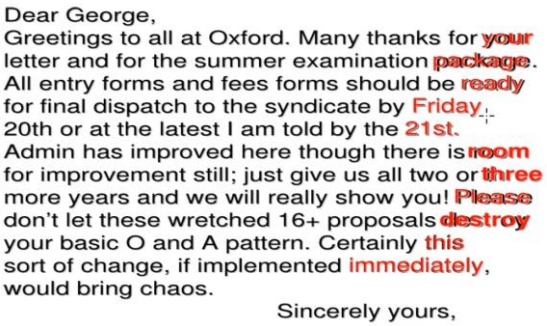



- Mám grayscale alebo rgb obrázok a chcem ich vytlačiť na lejzrovej alebo atramentovanej tlačiarni
- Netlačí ich priamo, ale rozbíja obraz na bodky a bodkuje ho, podľa tmavosti pixelu sa vybodkuje obraz
- Zakódujem nejakou kombináciou jednotku a nejakou inou nulu, ale tak aby sa bodky neprekrývali



## Steganografia v texte

- Základom je použitie štandardne vysádzaného textu
- Následne zložím správu zo slov, ktoré sa v ňom nachádzajú a mierne ich posuniem, na základe analýzy chýb vo vysádzaní som schopný dešifrovať správu


Dear George,
Greetings to all at Oxford. Many thanks for your letter and for the summer examination package. All entry forms and fees forms should be ready for final dispatch to the syndicate by Friday 20th or at the latest I am told by the 21st. Admin has improved here though there is room for improvement still; just give us all two or three more years and we will really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.
Sincerely yours,

## Útoky

- Bežný spôsob útoku je skôr vodoznak zničiť než odstrániť
- Napr. trochu otočím, trochu orežem a trochu zmením kontrast – toto by zrušilo všetky predstavené vodoznaky