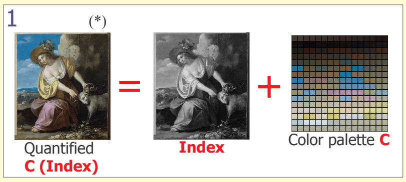
ATTACK BY COLORIZATION OF A GREY-LEVEL IMAGE HIDING ITS COLOR PALETTE

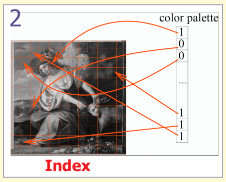
Marc CHAUMONT and William PUECH
marc.chaumont@lirmm.fr and william.puech@lirmm.fr
LIRMM, UMR CNRS 5506, Université de Montpellier II

HIDING COLORS; PALETTE-BASED SCHEMES:

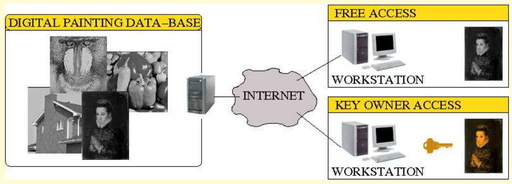
PRINCIPLE:

1. Find an index image and a color palette with:
   - A **color quantized image** close to the **color image**
   - An **index image** close to the **luminance image**
   - A **color palette** owning **consecutive couple of close color**
2. Embed the color-palette into the index image





WHY HIDING COLOR INFORMATION ?



COLOR SECURED of image database.
↳ free access to grey-level images,
↳ key-manage access to the color information.

« *A Grey-Level Image Embedding its Color Palette* », *ICIP'2007*
« *A Fast and Efficient Method to Protect Color Images* », *VCIP'2007, SPIE'2007*

IS IT EASY FOR AN ATTACKER TO RETRIEVE THE COLOR PALETTE ? … knowing the watermarked index image

PROBLEM FOR THE ATTACKER:

Retrieve the color palette *C* knowing the (waternarked) *Index* image.

ATTACKER HYPOTHESIS:

Two spatially close pixels i and j should own a similar color if their intensity are similar.

MATHEMATICAL MODEL, minimize for each pixel i:

$$\sum_{j \in \mathcal{N}(i)} w_{i,j}.(C(Index(i)) - C(Index(j)))^2$$

with $w_{i,j}$ a weighting value;
$w_{i,j} \approx 1$ when Index(i) ≈ Index(j)
$w_{i,j} \approx 0$ when Index(i) ≠ Index(j)

GENERAL COST FUNCTION TO MINIMIZE:

The attacker manually sets L couples (i_l, c_l)
where i_l is a pixel position and c_l its associated color.

$$E(C) = \sum_{i=1}^{N} \sum_{j \in \mathcal{N}(i)} w_{i,j}.(C(Index(i)) - C(Index(j)))^2 + \lambda \sum_{l=1}^{L} (C(Index(i_l)) - c_l)^2.$$

For each color k ∈ [1,K]:

$$C(k) = \begin{cases} \frac{\lambda.c_l + N(k)}{\lambda + D(k)} & if\ \exists l,\ Index(i_l) = k, \\ \frac{N(k)}{D(k)} & if\ \nexists l,\ Index(i_l) = k \end{cases} \quad (1)$$

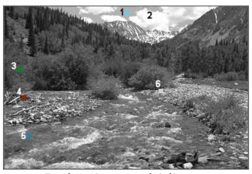
$$N(k) = \sum_{i | Index(i)=k} \left(\sum_{j \in \mathcal{N}(i)\ and\ Index(j) \neq k} w_{i,j}.C(Index(j)) \right) + \sum_{i | Index(i) \neq k} \left(\sum_{j \in \mathcal{N}(i)\ and\ Index(j) = k} w_{i,j}.C(Index(i)) \right)$$

$$D(k) = \sum_{i | Index(i)=k} \left(\sum_{j \in \mathcal{N}(i)\ and\ Index(j) \neq k} w_{i,j} \right) + \sum_{i | Index(i) \neq k} \left(\sum_{j \in \mathcal{N}(i)\ and\ Index(j) = k} w_{i,j} \right)$$

Colorization Algorithm (Minimization of E):

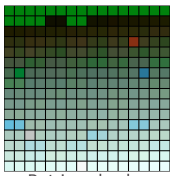
```
const Integer NBITER; // maximum number of iteration

Procedure Colorization(): Palette
begin

  Palette Cnew, Cold; // current and previous color palette

  // TAKE INTO ACCOUNT THE L USER COLORS ;
  // ∀l ∈ [1, L], Cnew(Index(i_l)) ← c_l
  init(Cnew);

  // ITERATIONS
  loop until NBITER reached or CONVERGENCE reached
  begin

    // COPY Cnew INTO Cold
    Cold ← Cnew;

    // UPDATE THE PALETTE Cnew WITH Cold KNOWLEDGE
    Apply equation 1;

    // SET IN CONFORMANCE EACH COLOR Cnew(k)
    // (U and V pixels ∈ [0, 255])
    conformance(Cnew);

  end

  // RETURN PALETTE
  return Cnew;
end
```

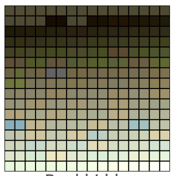
RESULTS AND CONCLUSIONS:

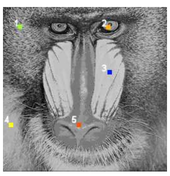

Index image hiding a color palette


Colorization attacked image


Rebuilt image knowing the secret key


Retrieved color palette


Real hidden color palette


Index image hiding a color palette


Colorization attacked image


Rebuilt image knowing the secret key

Conclusion:

- A **new indirect attack** specific to color-hiding schemes,
- A **fast** and **quasi-automatic** algorithm producing **pleasant color images**,
- An easy way to **illegally print color versions** of grey-level images.

↳ Future schemes should take this attack into account !

Acknowledgments: *TSAR French Project ANR SSIA 2006-2008*

(*) Saint-Germain-en-Laye museum; « *a young woman holding a ram* », Jan van Bylert (1603-1671), oil on oak.