Crop-Resistant Watermarking with Binary Images

NSF REU Program
Watermarking

• Watermarking is an important security tool.
• In a full color or grayscale image, pixels can be changed by an imperceptible amount.
• In a binary image, a pixel is either black or white, so there are no subtle changes.
What can we do?

- Divide the image up into $n$ sections, where $n$ is the number of bits you wish to encode.
Encode with Parity

- Each section has either an even or odd number of black pixels in it. Change a pixel in each section to encode.
Problem!

- Some of the sections have no pixels that are easy to change.
- We “shuffle” the pixels.
Some pixels can be changed more easily than others.
Use a Rubric

- This image shows the pixels that one method finds very flippable.
Commence the Watermarking

Original Image

50 bits embedded – Almost the same

250 bits embedded – Visible Artifacts
Other kinds of images

Lolcats are image macros combining photographs of a cat with a humorous and idiomatic remark, derived from lol and cat.[1][2] The phenomenon is also referred to as Caturday by users of 4chan, an online forum for sharing imageboards and other internet forums. Lolcats' popularity continues to grow, and the cuteness of cats "enhances" the appeal and increasing prominence of these drawings.

The term "lolcat" gained national attention in the United States when it was covered by major newspapers.[3] These phenomena of the sort are increasingly rare, stating that lolcats have "a distinctly old-school feel."[4] These images usually consist of a photo of a cat with a large caption characteristically."

The image is, on occasion, digitally edited for effect. The caption generally acts as a sort of semi-realistic description of the depicted scene. The caption is intentionally written with deviations from normal English spelling and grammar, including strangely-conjugated verbs, but with a tendency to converge to a new set of rules in spelling and grammar, referred to as a type of pidgin or baby talk.[13] The text parodies the grammar-poor style of the original caption. Lolcat captions take the form of snowclones in which nouns and verbs are replaced in a way that seem to be specific to the lolcat form. Common themes include jokes of the form "I'm in trouble/ I'm in my parents' room/ I'm in my room/ I'm in trouble..." and "I'm not doing anything..." Other themes are often derived from clips of music videos or other videos featuring cats.

30 bits are hidden –
some fonts are very regular,
Reducing the density of
Information that can be hidden.

This drawing has lots of
Edges, so lots of data can
Be hidden invisibly
Hidden Information

John Hancock
Translation and/or Cropping!
Traps the Hidden Info

- In a translated image, nothing is in the right subsection any longer, so the decoding produces something unrelated to the message.
- In a cropped image, the deshuffling process breaks because the image isn’t even the right size.
Can we fix it?

- Add a step to the encoding process.
- Will find ‘anchor points’ unlikely to be affected by watermarking or minor attacks.
- Keep track of shuffling map and anchor points in terms of a focus point selected for uncroppability, not a corner point.
Where’s the Focus?

- The focus point is the point that we will use as 0,0.
- Slight benefits later if it’s something that won’t get cropped.
Anchor Picking

- Anchor points can be selected before or after watermarking. (After is slightly better.)
What to Retain?

- We need to retain three things about each anchor point: its color, and its vertical and horizontal offsets from the focus point.
- We will use these to test potential focus points.
Anchor Picking

- When the image is translated, we can use the anchor points to relocate the focus point.
- Don’t need very many. More increases accuracy, but is actually slower.
Re-Centering the Image

- We have a set of anchor information. We will test each point in the cropped image to see if it is a good candidate focus point.
- Candidate focus points are ranked according to how many anchor points match. If no distortion occurred except for the cropping, they should all match.
Questions?