

Robustness and Security of Digital Watermarks


By:

"L.R Matheson, S.G.Mitchell,
T.G. Shamoon, R.E.Tarjan, F.Zane"
STAR Lab, InterTrust Technologies Corporation

"A body of work exists [which is] devoted to answering the question of whether truly secure watermarks can exist, and what the characteristics of such marks might be."

presented by: Fariba Shadabi

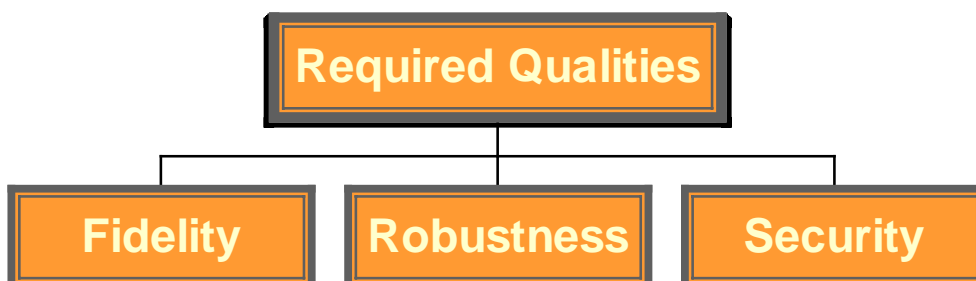
Outline

- **About Digital Watermarking**
- **Technical Challenges Faced by Watermarking Methods**
 - Fidelity (Briefly discussed in this paper)
 - Robustness 
 - Security (Not Presented)
- **The Components of a Watermarking System** (Not presented)
- **Conclusion**

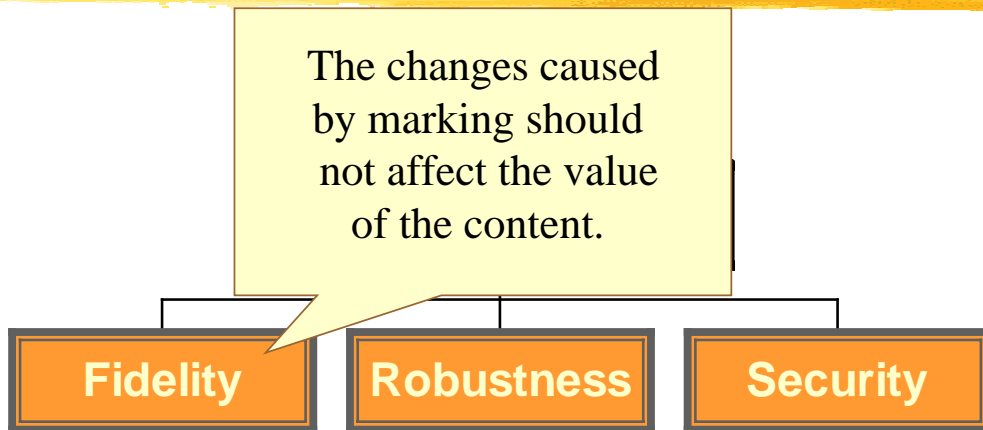
About Digital Watermarking

- Cryptography is a standard and Well-studied technical approach to reducing piracy.
- Digital Watermarking is a complementary approach that offers protection of unencrypted digital content.
- Since new technologies offer cheap and easy copying and distribution of pirated material, Robustness and Security of watermarks is receiving increasing attention.

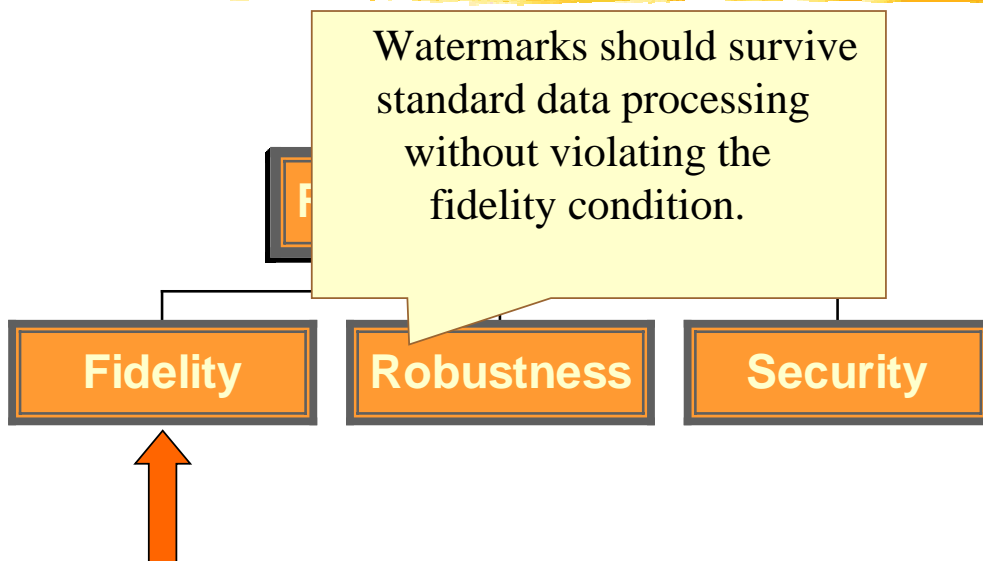
Technical Challenges Faced by Watermarking Methods



Technical Challenges Faced by Watermarking Methods

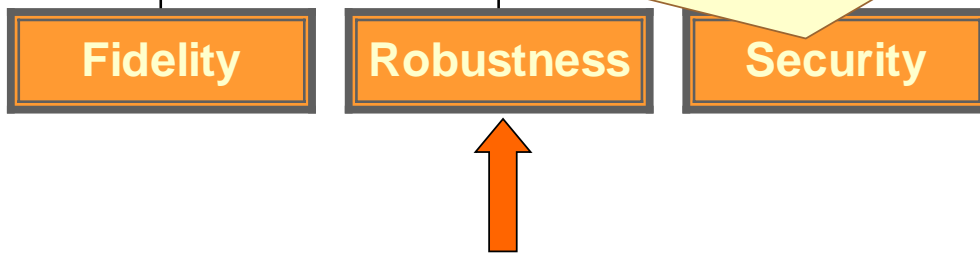


Technical Challenges Faced by Watermarking Methods



Technical Challenges Faced by Watermarking Methods

Watermarks should survive any planned attempts to remove them. An Attacker can try standard processing techniques plus other transformation techniques which are specifically designed to erase watermarks.



Robustness

- A Watermark should be robust, it must survive two types of standard processing techniques:

1) Alignment-preserving transformations

Include: Data compression, Data conversion, and others.

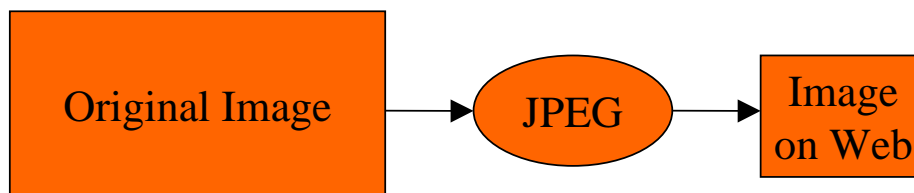
2) Alignment-altering transformations

Include: Cropping, Scaling and Rotation.

“ Digital Watermarks often Fail on Web Images ”

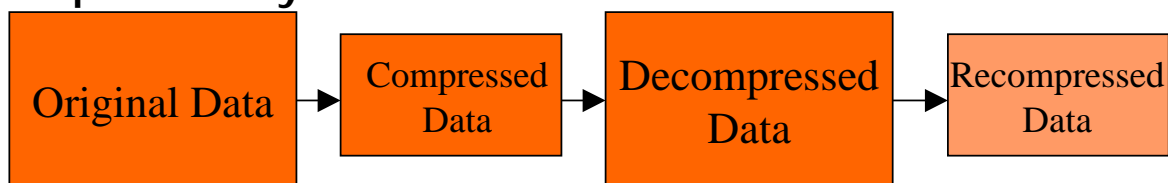
New York Times, 11 Nov 1997
By: Marty Katz

- Digimarc’s watermarking system (PictureMarc) often fails to leave a recognizable watermark on the kinds and sizes of images used most often on the Web.
- Factors that appear to have caused this problem:
 - The file size wasn’t big enough (need certain minimum picture file size to have enough bits of data/pixel to be encoded)
 - Web designer reduced the watermarked image’s size
 - JPEG compression



Surviving alignment-preserving transformations

- An audio watermarking algorithm has been proposed, it allows reading a watermark from the compressed data, but whether such watermarks survive decompression remains to be tested practically.



- Current watermarking methods offer possibly acceptable robustness against Alignment-preserving transforms but are not robust enough against altering transforms.

Surviving alignment-altering transformations

- Align a transformed watermarked image against the original, using pattern matching methods.
- Add a universal registration mark and align a transformed marked image against the registration mark.
- Do a self-alignment of transformed image, based on some set of distinguishable features.

Conclusion

- Digital watermarking is a young but rapidly growing technology.
- Currently watermarking are not robust enough against altering transforms.
- Whether all the theoretical approach in this field will lead to robust, practical watermarking schemes remains to be seen.
- This paper is very well-written and easy to understand.
- The authors made considerable effort to show the landscape of current digital watermarking.



Question

- Name a few factors which are important for watermarks surviving?

- Choosing a file with right size

- The right places
 - The right subset of the components must be chosen to be marked.