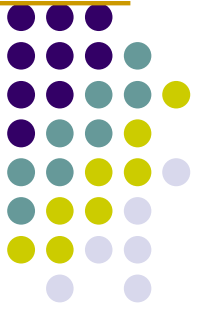


CryptMark: A Novel Secure Invisible Watermarking Technique for Color Images

Saraju P. Mohanty
VLSI Design and CAD Laboratory
Computer Science and Engineering
University of North Texas.
Email: smohanty@unt.edu



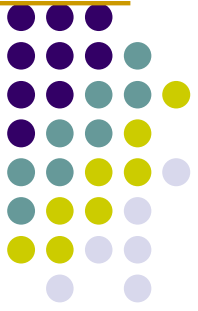
Outline of the Talk



- Introduction
- Related Research Work
- Contributions of this Paper
- The Proposed Approach
- Experimental Results
- Conclusions



DRM ?



- ❑ Digital Rights Management (DRM) is a generic term that refers to any of several technologies used by publishers, creators, or owners to control access and usage of digital data.
- ❑ Typically a DRM system:
 - Protects intellectual property by **encrypting** the data so that it can only be accessed by authorized users.
 - and/or
 - Marks the content with a digital **watermark** so that the content can not be freely distributed.

DRM ? ...

Watermarking

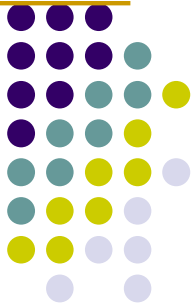


Cryptography



- ❑ Judicious use of both encryption and watermarking necessary for multilayer protection through DRM.

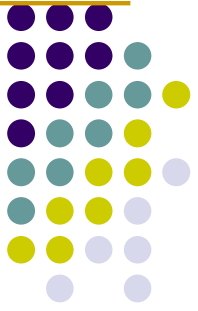
DRM : Objectives



- Whose is it?
- Is it tampered with?
- Where was it created?
- Who had created it?
- ... and more.



Digital Watermarking ?

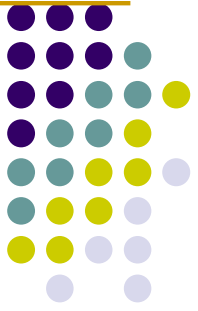


Digital watermarking is a process for embedding data (watermark) into a multimedia object for its copyright protection and authentication.

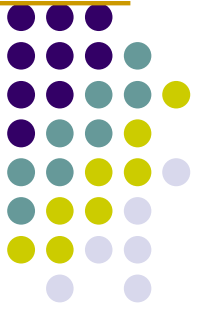
Watermarking Types:

- ☐ Visible and Invisible
- ☐ Spatial/DCT/ Wavelet
- ☐ Robust and Fragile

An Watermarked Image (from IBM)

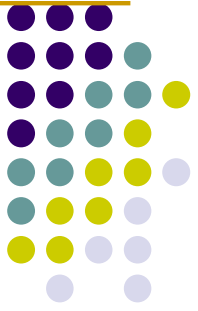


Related Research Works



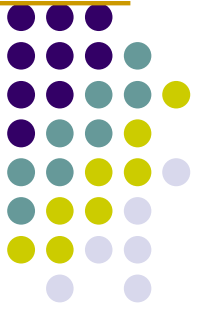
- ❑ **Sheppard, Naini, and Ogunbona – 2001:** Discuss techniques for embedding multiple watermarks into one multimedia object.
- ❑ **Jiang, Yu, Shi, Liu, and Kim – 2002:** DCT domain blind watermarking schemes adaptive to HVS.
- ❑ **Guo and Georganas – 2003:** Algorithm using generalized secret sharing scheme in cryptography to address joint ownership problem.

Related Research Works ...



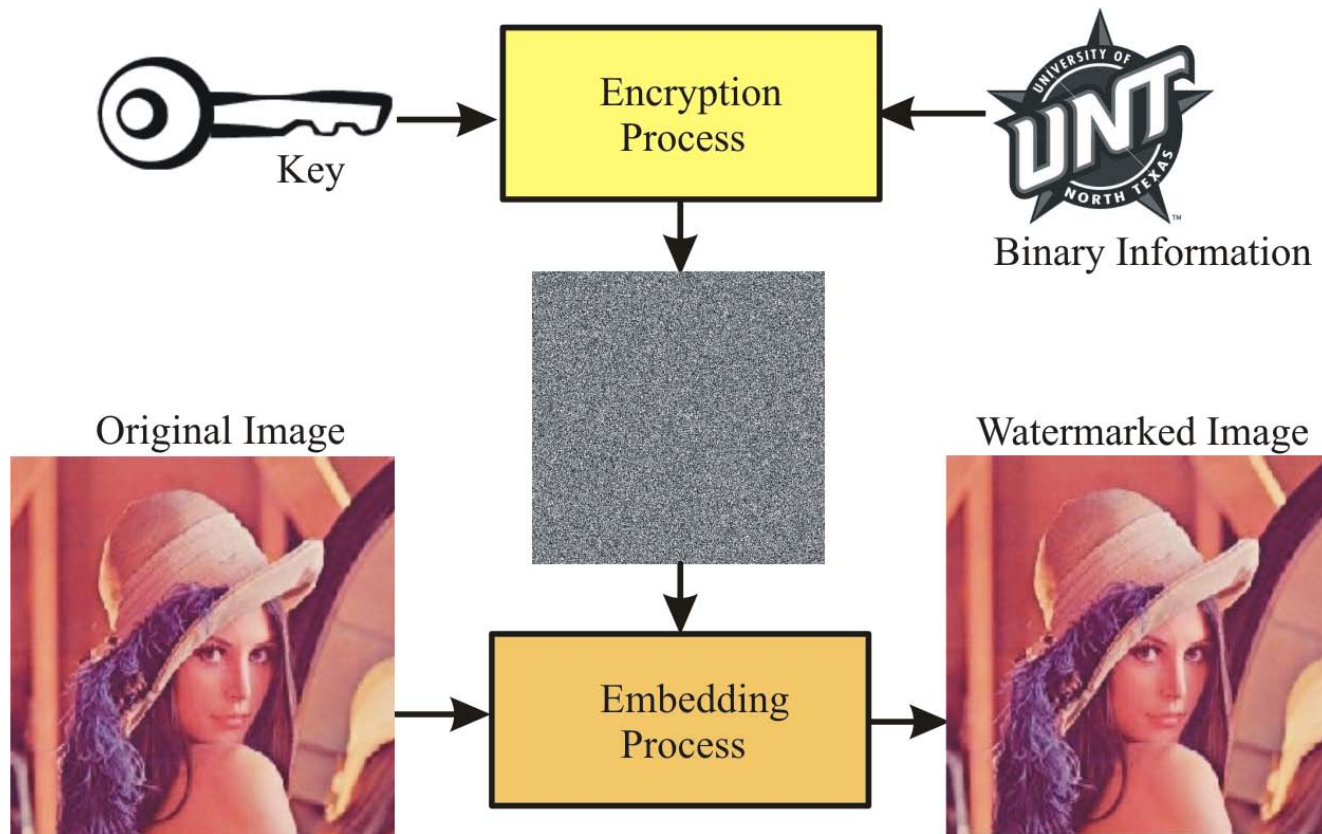
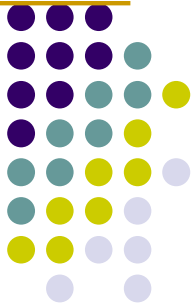
- ❑ **Lu, Xu, and Sun – 2005:** A multipurpose fragile-robust watermarking technique based on the multistage vector quantizer structures is presented.
- ❑ **Pai, Ruan, and Gotze – 2005:** Energy efficient DCT-based high performance watermarking algorithm is presented.

Novel Contributions of the Paper

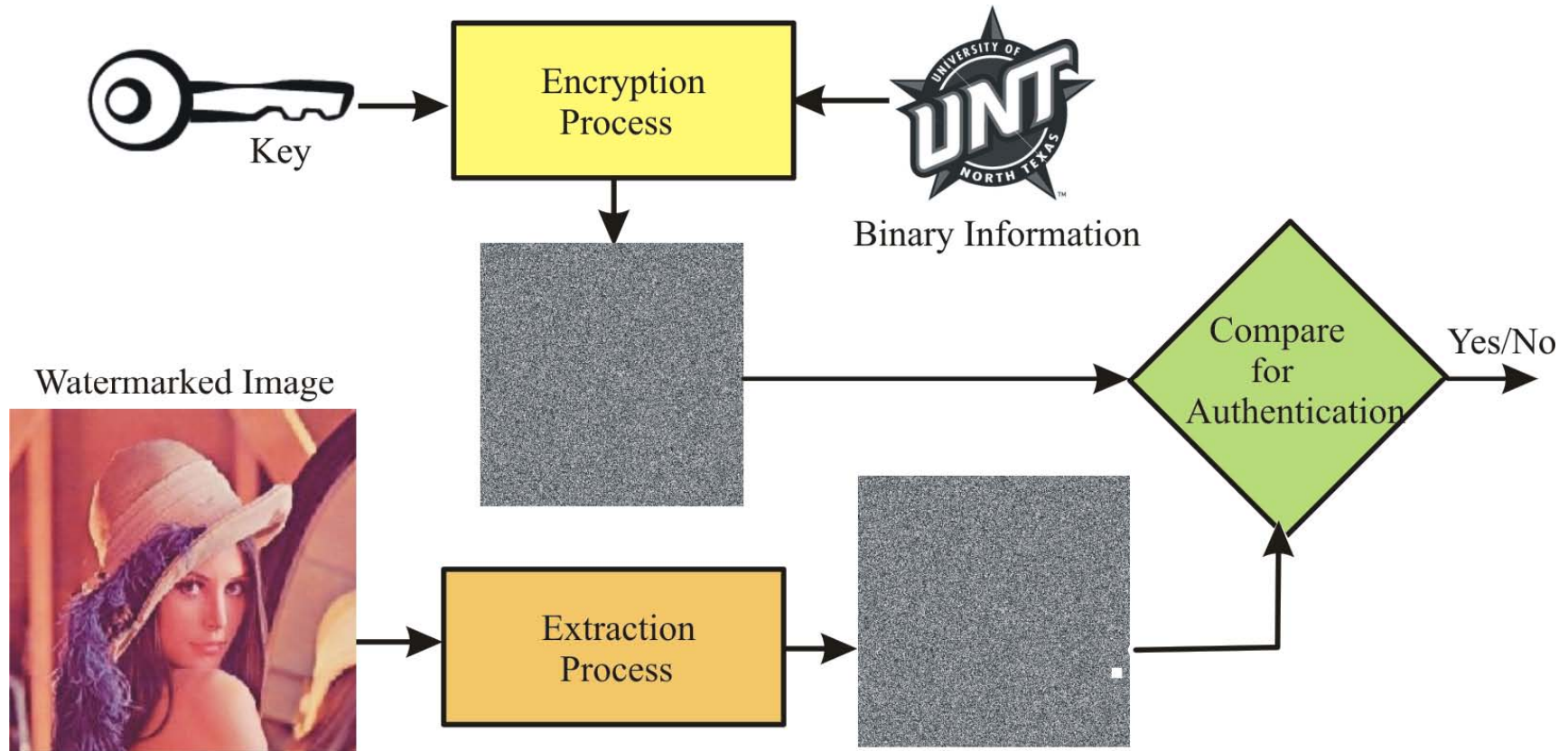
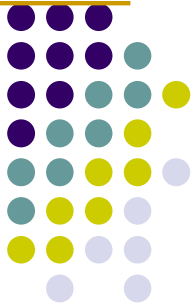


- ❑ A novel invisible watermarking method that uses cryptography and watermarking.
- ❑ **Security:** The *advantage* of encrypted watermark processing is that at no point of time raw watermark information is passed, thus providing security.
- ❑ **Attack Resilience:** Unlike most of the existing algorithms who heavily rely on low frequency AC components, this approach uses both DC and AC DCT coefficients.

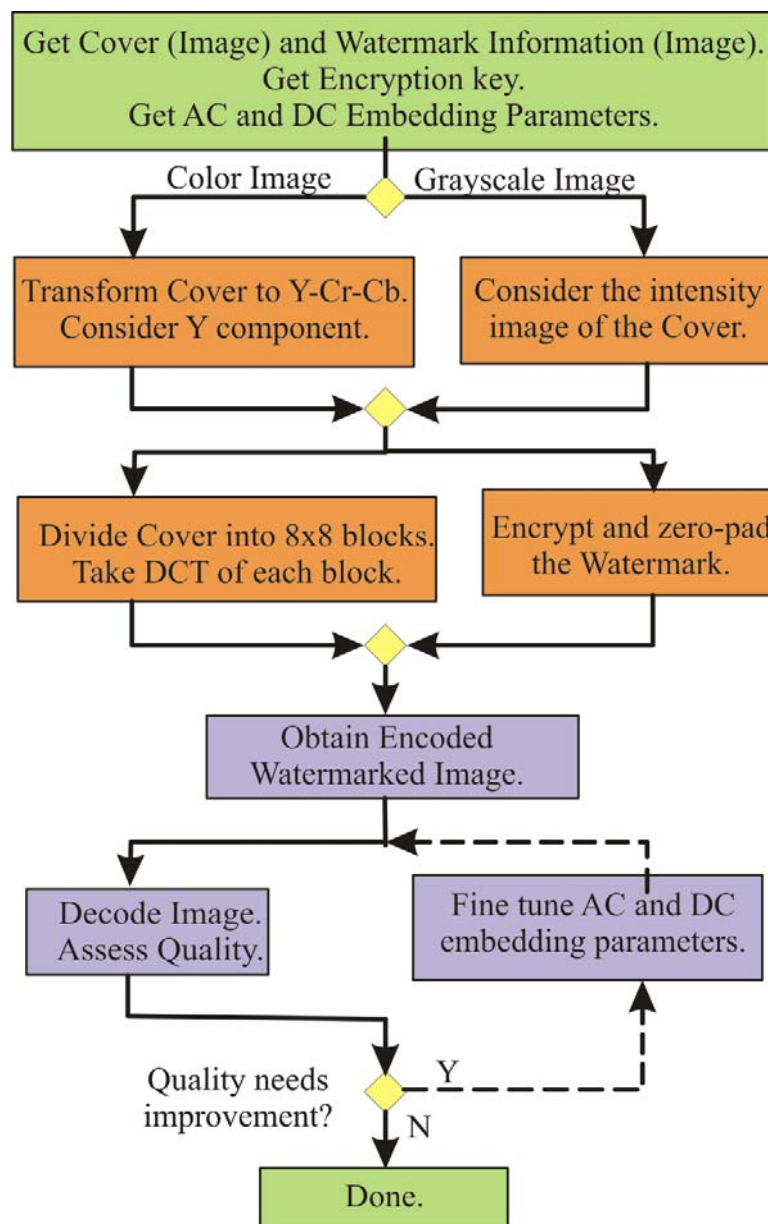
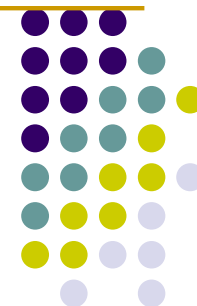
Proposed Approach: Insertion



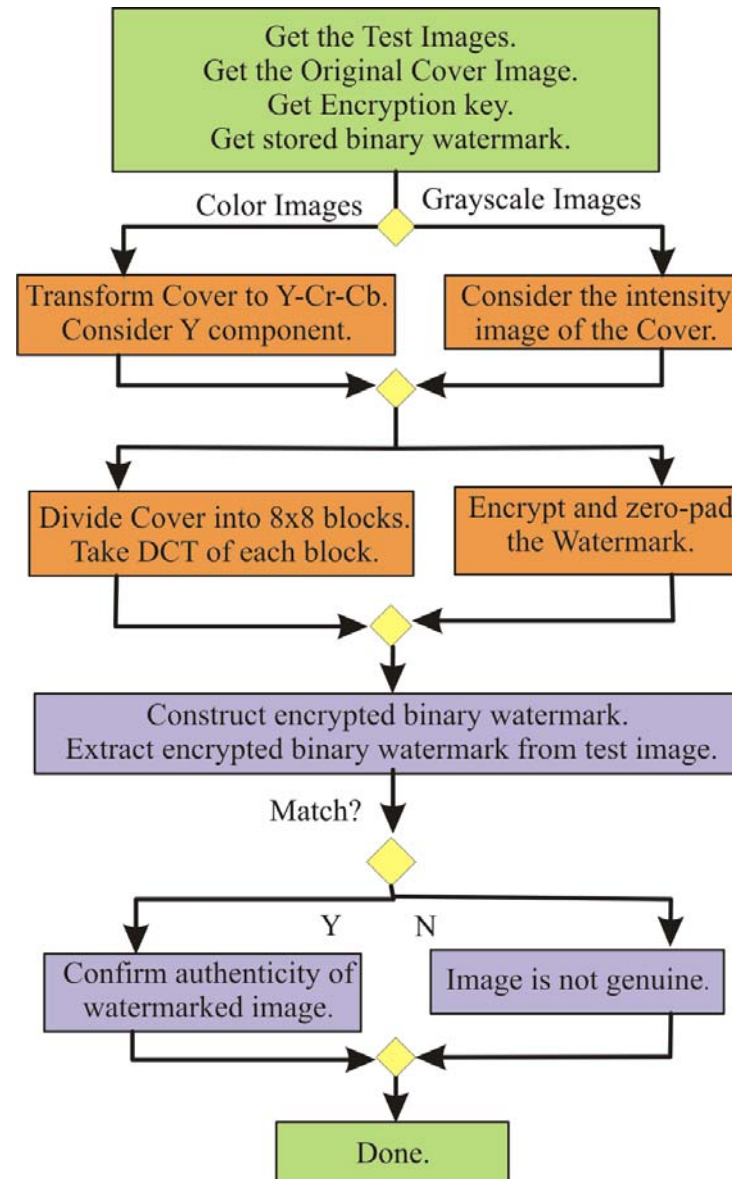
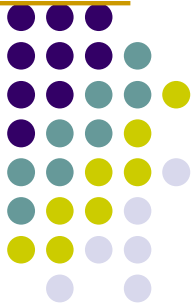
Proposed Approach: Authentication



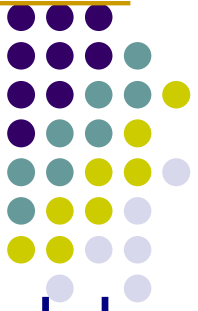
Algorithm Flow for Secure Insertion



Algorithmic Flow of the Extraction and Authentication



Insertion Operation



□ $c_{ij}(k)$ and $w_{ij}(k)$ denote values at position (i,j) of block k .

□ Watermark is embedded in cover image using:

$$c'_{ij}(k) = \begin{cases} c_{ij}(k)(1 + \alpha_{ij}) & \text{if } w_{ij}(k) = 1 \\ c_{ij}(k)(1 - \alpha_{ij}) & \text{if } w_{ij}(k) = 0 \end{cases}$$

□ Two embedding factors used:

- α_{dc} for DC components α_{00} .
- α_{ac} for AC components α_{01} , α_{10} , and α_{11} .

□ The values of α_{dc} and α_{ac} are chosen for a specified SNR threshold.

Extraction and Authentication Operation.

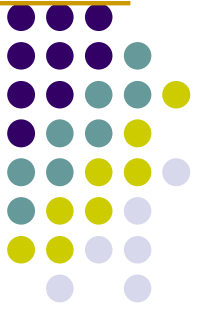


- ❑ $w_{ij}(k)$ and $w'_{ij}(k)$ original and extracted watermark blocks.
- ❑ Construct watermark using:

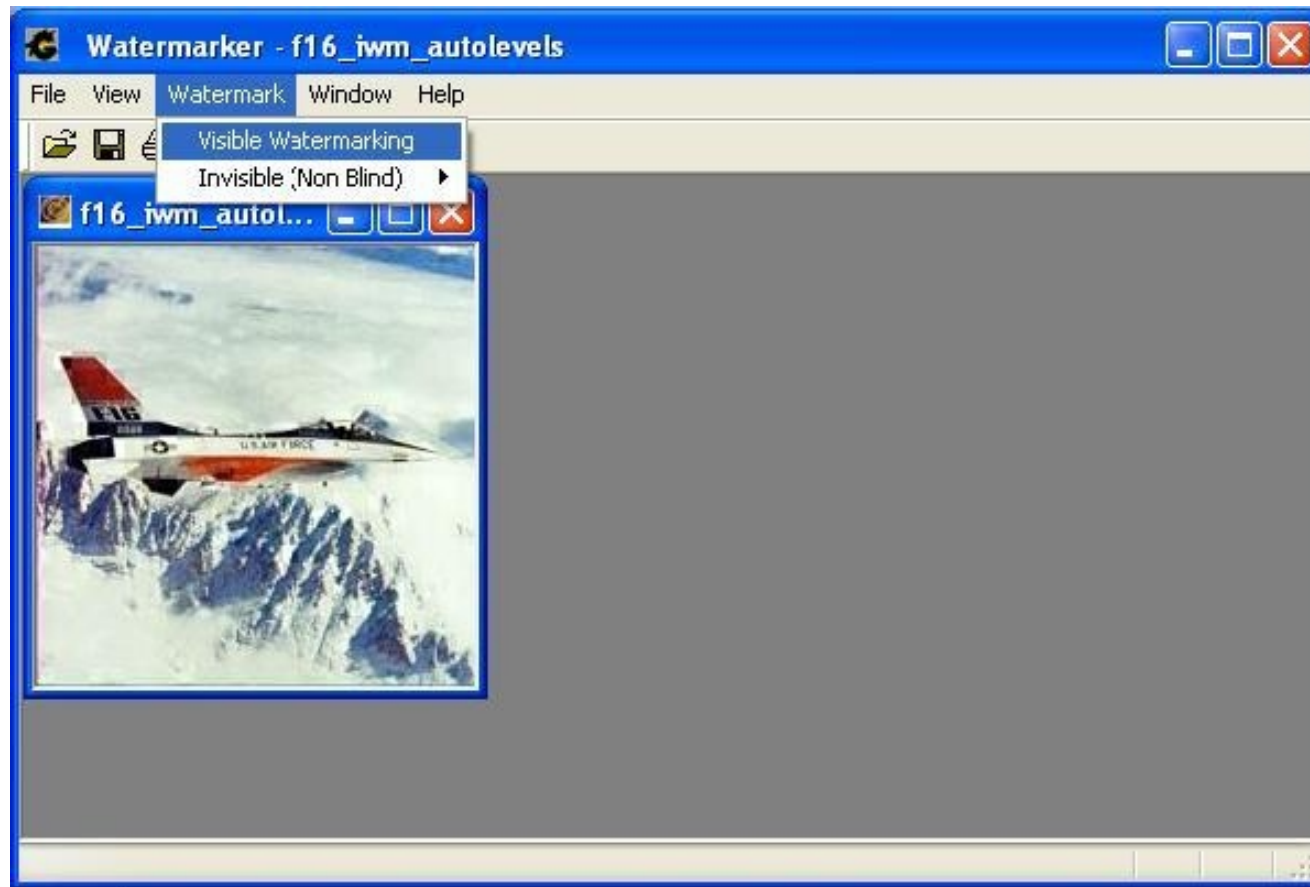
$$w'_{ij}(k) = \begin{cases} 1 & \text{if } c'_{ij}(k) > c_{ij}(k) \\ 0 & \text{otherwise} \end{cases}$$

- ❑ Compare $w_{ij}(k)$ and $w'_{ij}(k)$ for authentication.

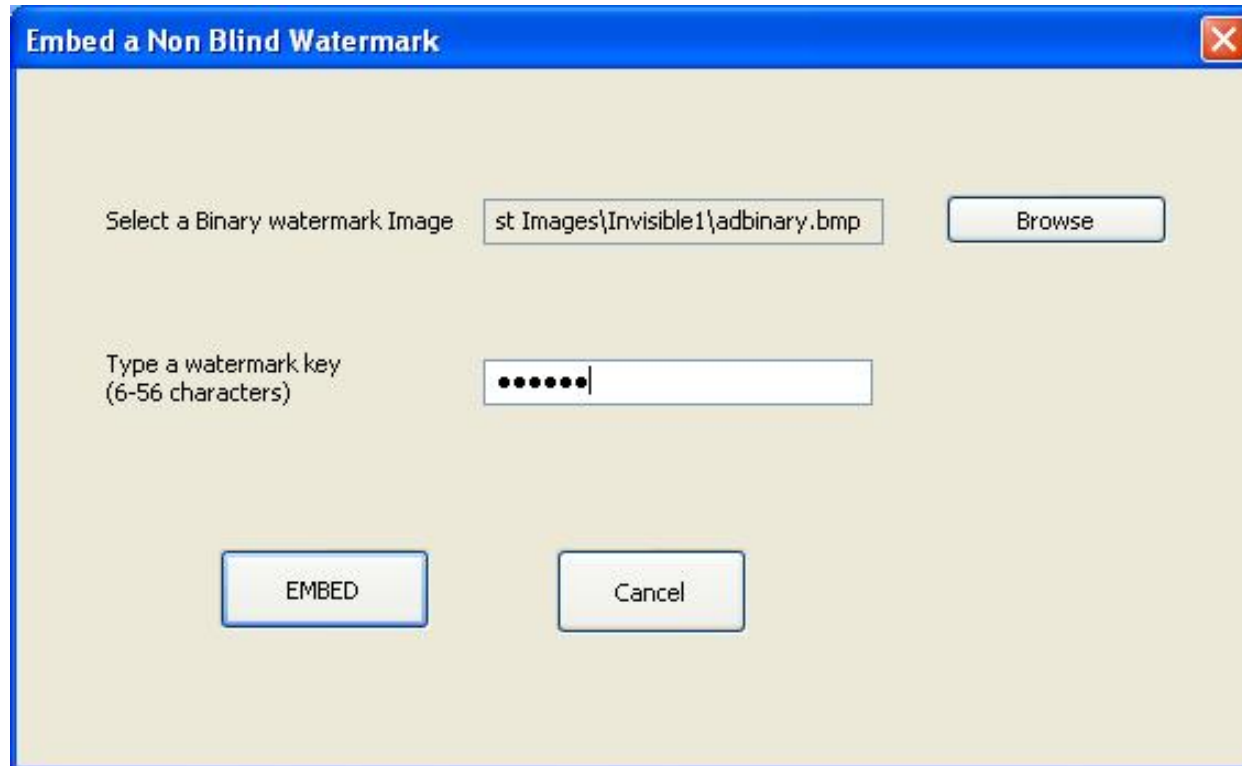
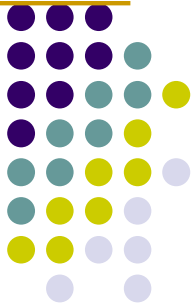
System Implementation: ISWAR (Imaging System with Watermarking and Attack Resilience)



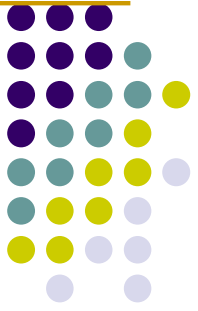
❑ **Available at:** <http://www.cse.unt.edu/~smohanty/ISWARwatermarker/>



System Implementation: ISWAR ...



Experimental Results: Test Images



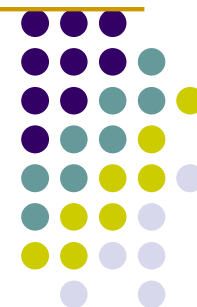
Original



Watermarked



Experimental Results: Performance



Attacks Performed for Testing	For Various Test Image		
	Lena (SNR = 105)	F16 (SNR = 99)	mandril (SNR = 101)
JPEG Compression 0 quality	Survived	Survived	Survived
Gray scaling 16 levels	Survived	Survived	Survived
Gray scaling 256 levels, JPEG compression 0 quality	Survived	Survived	Survived
Blurring , 0 quality JPEG Compression	Survived	Survived	Survived
Partial cropping	Survived	Survived	Survived
Stirmark Self Similarities	Survived	Survived	Survived
Stirmark 0 quality JPEG compression	Survived	Survived	Survived
Stirmark median filtering	Survived	Survived	Survived
Stirmark Random Distortions	Survived	Survived	Survived

Conclusions



- ❑ A novel invisible watermarking method called CryptMark is presented that uses cryptography and watermarking simultaneously.
- ❑ CryptMark can be an effective technique for DRM.
- ❑ Exhaustive testing of proved that the algorithm works well and can survive various forms of attacks.
- ❑ A possible extensions include use of wavelet transforms for embedding of strong watermarks.
- ❑ Blind extraction of watermarks is also a planned extension particularly because of its usefulness in authentication at the receiver end as well as identification of secretive communication.
- ❑ Low-power version of the watermarking scheme is also planned to be developed.



Thank You

For more information:

<http://www.cse.unt.edu/~smohanty>

