

# Designated Verification of Non-invertible Watermark

---

**hyejoung yoo**

Graduate School of Information Security, Korea Univ. Seoul, Korea  
[hjyoo@cist.korea.ac.kr](mailto:hjyoo@cist.korea.ac.kr)

# abstract

- ◆ copyright protection & authentication
- ◆ designated verification of undeniable signature so that the confirmer of watermark can sure that only intended verifier(s) can be convinced about the validity or invalidity of the signature.
- ◆ more secure watermarking method while keeping efficiency of well-known class of watermarking schemes ; re-watermarking attack

# Intro.

- ◆ Digital material has very dangerous environment.
- ◆ Encryption
- ◆ Properties :
  - imperceptibility
  - inseparability
  - undergo the same transformations as the Works
- ◆ Applications :
  1. Signatures
  2. Fingerprinting
  3. Authentication
  4. Copy control or Device control
  5. Secret communication

- ◆ problems :

- S. Craver, "Resolving Rightful Ownerships with Invisible Watermarking Techniques:", 1998

- ♣ limit of the capacity of invisible watermarking schemes to resolve copyright ownerships

- : multiple claims of rightful ownerships

- undeniable signature scheme

- ◆ undeniable signatures

- : D. Chaum, "Undeniable Signatures", 1989

- : verifier is unable to distinguish between valid and invalid watermarks

- ◆ if the message in is copyright owner's information, it is non-invertible
- ◆ zero-knowledge based watermarking mechanism
  - : public enough to be detected yet private enough not to be removed
- ◆ - re-think approaches to invisible watermark
  - re-evaluate the promises
  - find cryptological means in order to protect rightful copyright owners more securely

## content

- ◆ 2 : present the overall digital watermarking mechanism
  - ◆ review the existing literature
- ◆ 3 : consider re-watermarking attack and its possible solution
- ◆ 4 : propose non-invertible verification process with commitment scheme
  - ◆ solve the problem of ambiguous resolution of ownership with the proposed watermark scheme
  - ◆ discuss the proof of ownership
- ◆ 5 : explain how practical it is
- ◆ 6 : consideration of the future works

# Digital Watermark

- Definition & Function
  - ◆ Visible vs. Invisible
  - ◆ Copyright protection vs. Data authentication
  - ◆ In this paper : one instance of ownership verification and identification of rightful owner(s)
  
  - ◆ Essential Property :
    1. recoverable despite intentional or unintentional modification of the content
    2. Invulnerable to the deliberate attempts to forge, remove, or invalidate watermark
  
  - ◆ Only labeling to the obtained content is vulnerable to the counterfeited attack.
  
  - ◆ Copyright protection : undeniable verification of original watermark embedder

## ■ Watermark Mechanism

◆ undeniable watermark

◆ notation

$I$  : image

$\{w_1, w_2, \Lambda, w_n\}$  : watermark

$I_w$  : watermarked image

$E$  : encoder

$D$  : decoder

$P(W)$ ,  $P$  : indicating function of presence of wm

$f_1(I), f_2(I), \Lambda, f_n(I)$  : derived feature

◆ overall embedding and recovery mechanisms

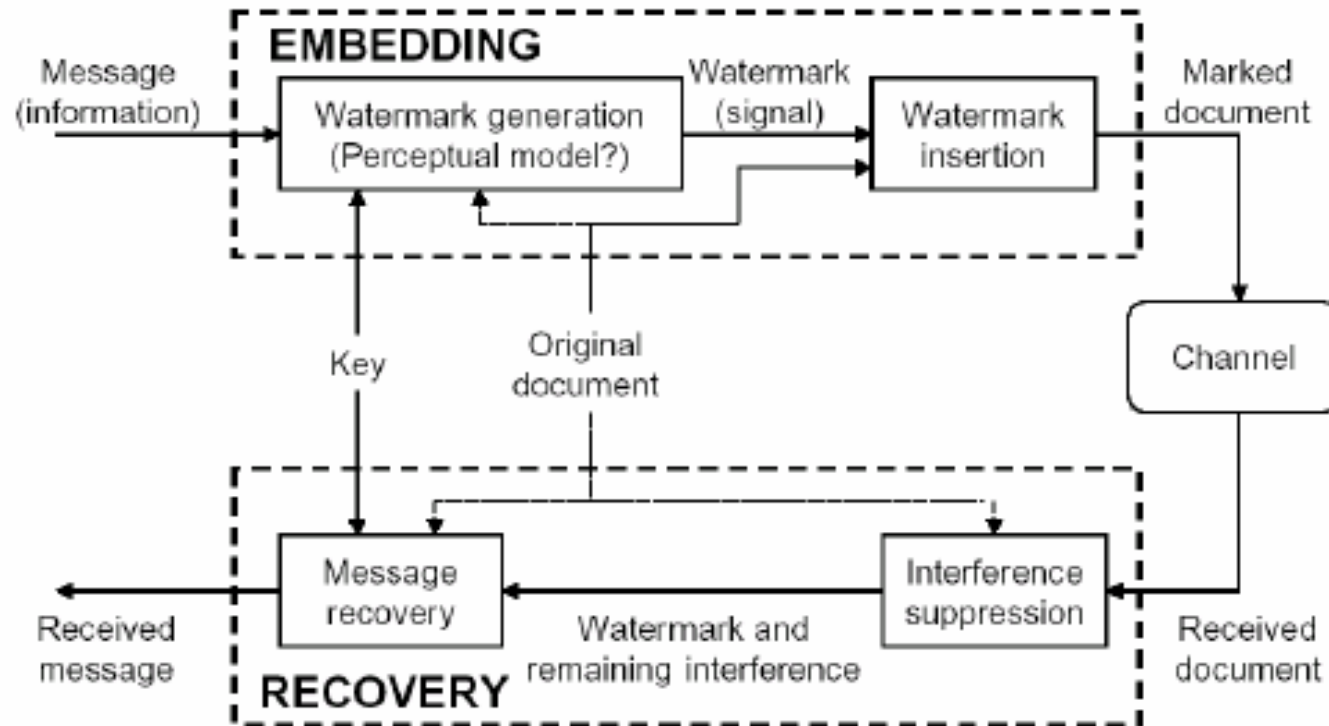


Fig. 1. Digital Watermark Module.

## ■ Watermark Verification

- ◆ GEN\_KEY
  - asymmetric watermarking scheme
  - symmetric watermarking scheme
  - un-keyed watermarking scheme
- ◆ GEN\_W
- ◆ E
- ◆ D

$I, k_{\text{det}})$

; informed detection vs. blind detection

- ◆ three watermarking mechanisms for digital data  $D'$

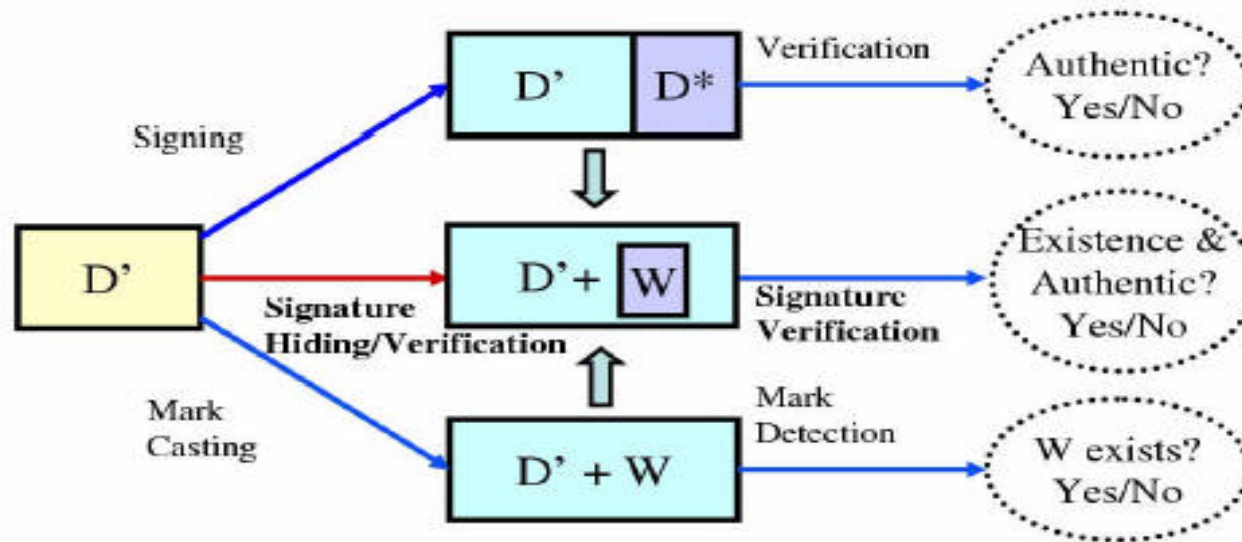


Fig. 2. Watermark Verification and Authentication Mechanisms.

- construct new hybrid mechanism on digital watermark verification and authentication system

# Attack & Its Solution

## ■ Re-watermarking Attack

- ◆ Q1 : How can we decide the original watermark?
- ◆ Q2 : How can we decide which watermarked version of an image is the truly watermarked version in circulation?
- ◆ S.Craver : two failing scenarios of resolving rightful ownerships
  - > solution : non-invertible watermark
  - > did not suggest the concrete protocol
  - > there are some unsolved problems

## ■ Solution : Undeniable Verification

- ◆ simply solved if we consider undeniability in watermark verification process

## ■ Undeniable Property of Digital Watermark

- ◆ from self-verification property
- ◆ to verification process with original watermarker
- ◆ using undeniable scheme in the watermarking process
- ◆ commitment mechanism : designated verifier certificate
- ◆ multimedia contents company for instant proof of product authenticity to their buyers
- ◆ individual who wishes to sign a data anonymously

- New Verification Mechanism

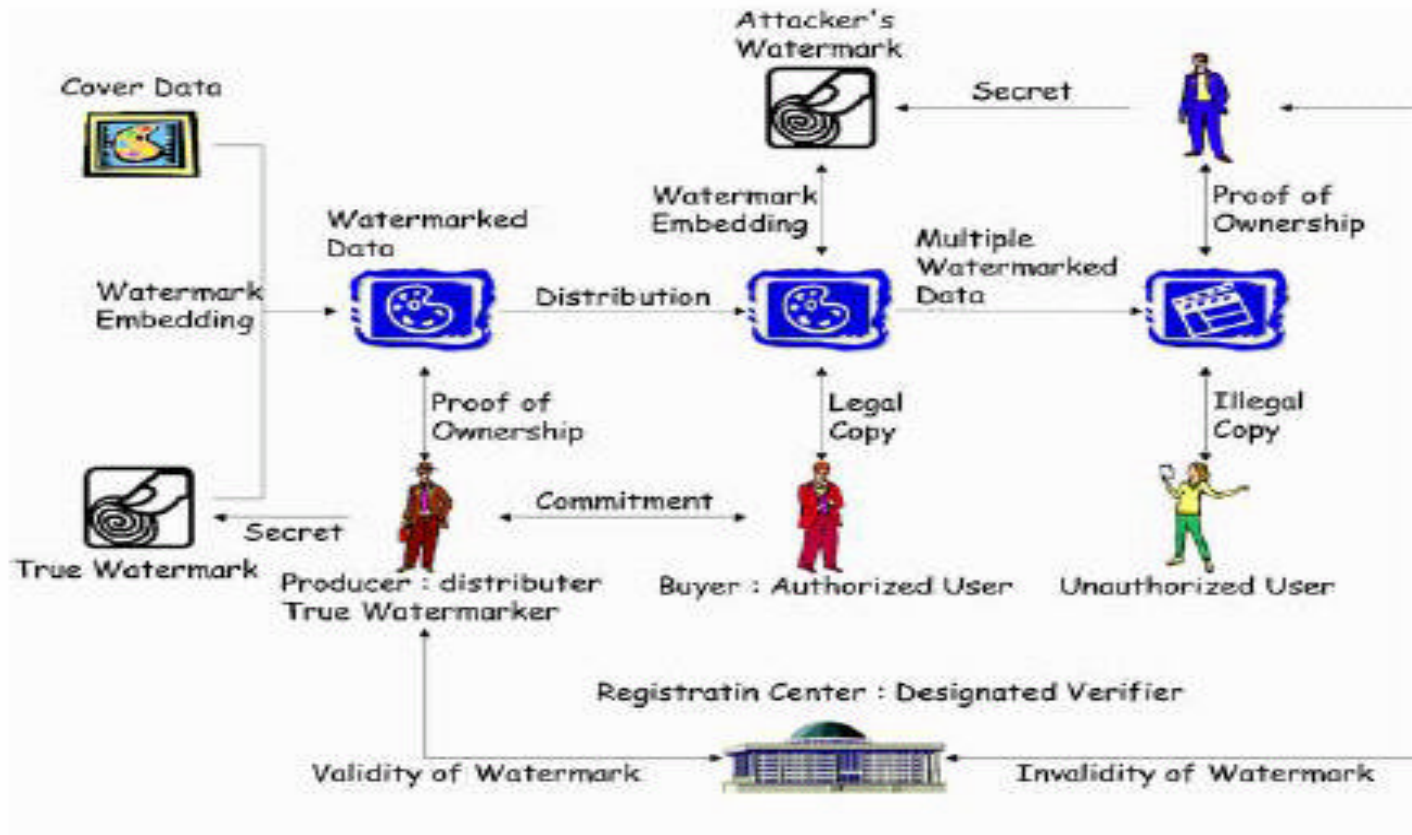


Fig. 3. New Watermark Verification Mechanism.

# Designated Verification for Undeniable Watermark

- ◆ Designated Verifier

$(P_A, P_B)$  : a protocol for Alice to prove the truth of the watermark to Bob

## ■ Commitment Scheme

- ◆  $(com, open)$
- ◆  $com(m, par\_com)$
- ◆  $open(com, par\_com, sk\_com)$
- ◆ security requirements
  - : binding(committing) & hiding(secretcy)
- ◆ harmonic property
  - : the committer can open  $com(m_1) * com(m_2)$  to  $m_1 + m_2$  without revealing additional information about the contents of  $com(m_1)$  &  $com(m_2)$ .
- ◆ additional trap-door one-way properties -> commitment mechanism + digital watermark verification procedure

## ■ Trap-Door Commitment

- ◆ trap-door primitives :  $c$  is trap-door commitment scheme if and only if followings hold

1. No polynomial-time machine can, given  $y_i$ , find a multiple  $(w_1, r_1)$ ,  $(w_2, r_2)$  such that  $c(y_i, w_1, r_1) = c(y_i, w_2, r_2)$ .
2. No polynomial-time machine can, given  $y_i$  and  $c(y_i, w, r)$ , output  $w$ .
3. There is a polynomial-time machine that, given any quadruple  $(x_i, w_1, r_1, w_2)$  in the set of possible quadruples, finds  $r_2$  such that  $c(y_i, w_1, r_1) = c(y_i, w_2, r_2)$  for the public key  $y_i$  corresponding to the secret key  $x_i$ .

◆ simple trap-door commitment scheme

1. Secret extracting (decryption) scheme from watermarked data :  $D()$ .
2. Public embedding (encryption) scheme for watermarked data :  $E()$ .
3. Value to commit to :  $w$  in  $\text{Range}(E)$ .
4. Commitment: Alice randomly selects  $r$  in  $\text{Range}(E)$ . And Alice calculates a commitment  $c = E(w) + E(r)$ , where  $+$  is a combiner such as XOR.
5. Decommitment: Alice sends Bob  $(w; r)$ .

◆ how to change the normal watermark verification scheme for undeniable verification -> designated verification for undeniable watermark system

## ■ Undeniable Verification with Commitment

- ◆  $(\text{com}, \text{open})$  : secure commitment scheme
- ◆  $(\text{GEN\_KEY}, \text{GEN\_W}, \text{E}, \text{D})$  : undeniable proof protocol between P & V
- ◆ common inputs of P & V :  $I^W, \text{com}(I), \text{com}(W), \text{com}(k_w)$
- ◆ private input of the prover :  
 $\text{sk\_com} = (\text{sk}^W_{\text{com}}, \text{sk}^I_{\text{com}}, \text{sk}^{kw}_{\text{com}})$
- ◆ P outputs a boolean value to the verifier



◆ procedure of watermarking

1. Generating & Processing a Key/Data
2. Generating & Embedding watermark
3. Constructing a Proof
4. Verifying a Proof

## Discussion :

### Proof of Ownership and Zero-Knowledge

- ◆ undeniable verification procedure
- ◆ proof of copyright or ownership of some resources by T or CA
- ◆ H:the owner of a work I' iff the following conditions hold
  - H has previously registered a new work I' on the trusted center T,
  - I is similar to I', and
  - I' is the first registered work to which I is similar.
- ◆ zero-knowledge watermark verification
- ◆ without revealing any information about the watermark, the reference data, and the detection key
- ◆ identification module + watermark verification

# Practicability of Our Scheme

- Cox et al.'s scheme
  - ◆ Structure of the watermark : i.i.d in  $N(0,1)$ ,  $\{-1,1\}^n$
  - ◆ Watermarking procedure : spread spectrum – the  $n$  highest magnitude DCT AC values
  - ◆ Inserting and extracting the watermark :  $v'=v(1+ax)$ ,  $a$  : scaling factor
  - ◆ Evaluating the similarity of watermarks :

$$\rho(X^*, X) = \frac{X^* \cdot X}{\sqrt{X^* \cdot X^*}}$$

- Practicability of our scheme

$$X^* = X$$

$X^*$  : retrieving watermark

$$X = \{\pm 1\}^{1000} \sim N(0,1)$$

$X$  : original watermark

$$m(X^*, X)$$

$$m(X, X)$$

$$\overline{X \cdot X}$$

$$\overline{X \cdot X}$$

$$x_i^2$$

- ◆  $W = m^x \cdot A \pmod{p}$
- ◆  $|W| \leq |p|$
- ◆ ECC signature module
- ◆  $|W| = 160$  bits

	similarity	recovery rate
no-error ( $X=X^*$ )	31.6	100%
image scaling	13.4	71.2%
10% quality 0% smoothing JPEG	22.8	86%
5% quality 0% smoothing JPEG	13.9	72%
clipping	14.6	73.1%

- ◆ consideration of computation recovery rate & size of the watermark
- > proposed scheme can sufficiently retrieve the undeniable watermark using error correcting code while keeping practicability

# Conclusion

- ◆ solve multiple watermarking problem as we consider it by the designated verification process.
- ◆ if there are multiple watermarked image, the original owner can cooperate with its verification process.
- ◆ propose undeniable verification scheme in the watermarking process on network-based secure contents distribution.
- ◆ using the designated verifier proof schemes, watermark can be verified by commitment methods.
- ◆ **future work**: zero-knowledge based designated verification mechanism



CONCLUSION COMMENT  
&  
THANK YOU

3rd Oct.03

ISC03 IN BRISTOL

28