$$\alpha = \frac{Z'_{target}}{Z_{lc}(w_s, w_m)}$$

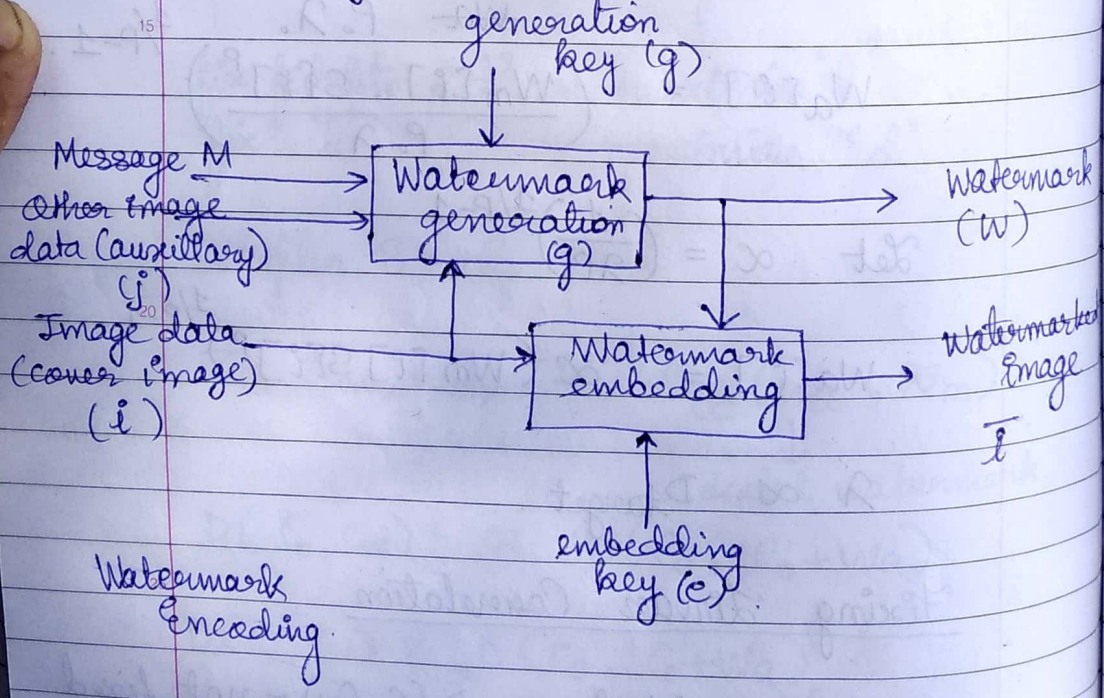
$$= \frac{Z_{target} - Z_{lc}(C_o, w_m)}{Z_{lc}(w_j, w_m)}$$

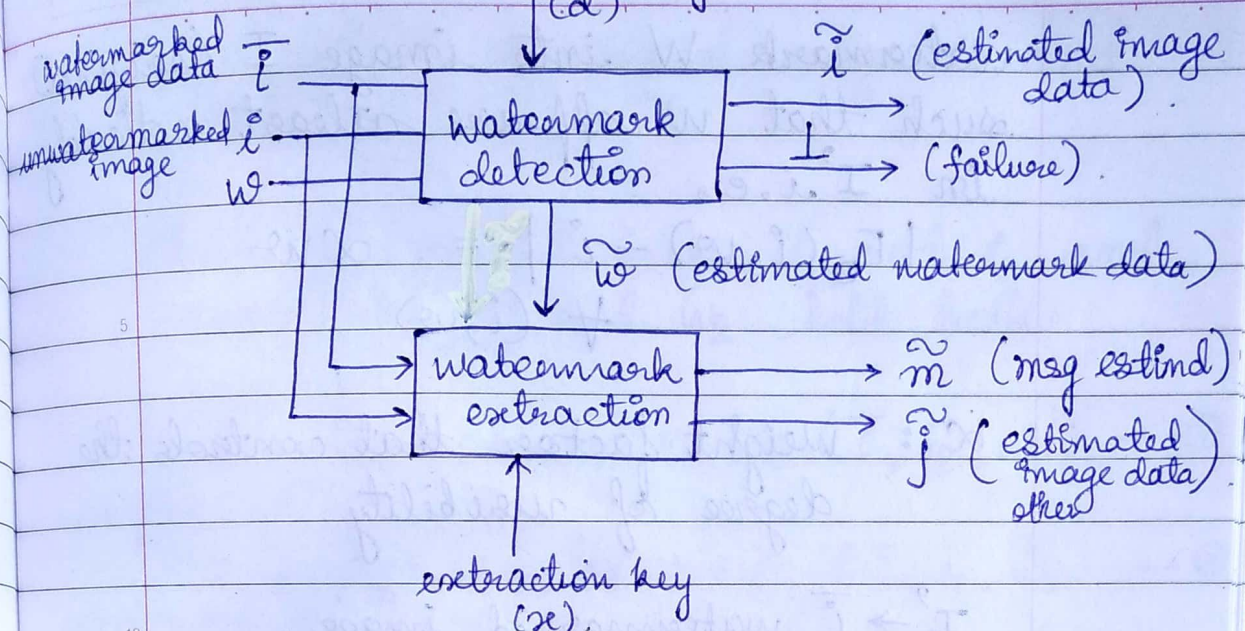
=

14.3.19.

Digital Image Watermarking, formal model fundamental properties

– Nyeem Etal.





Watermark decoding

Perceptual Similarity

Any two images i_1 and i_2 are said to be (d, t) perceptually similar if $d_j(i_1, i_2) \leq t_j$ for all similarity measures $d_j \in d$, thresholds $t_j \in t$.

$d \equiv \{ d_1, d_2, d_3 \dots d_n \}$ and threshold.

$t \equiv \{ t_1, t_2, t_3 \dots t_n \}$.

t is predefined

(d_j, t_j) perceptually similar

'n' measures of similarity.

Visibility

A watermarking scheme is called visible or perceptual if $E(\cdot)$ embeds a given

watermark W into image I (original) such that W appears atleast noticably in I' i.e.

$$|E_e(i, w) - i| = \alpha w \quad \forall (i, w)$$

α : weight factor that controls the degree of visibility.

$I' \rightarrow \bar{i}$ watermarked image.

$I \rightarrow i$ original image.

$E_e(i, w) = \bar{i}$

↓ embedding function

α is less. visibility is less.

A watermarking scheme is called invisible or imperceptible if E embeds w into i such that $\bar{i}$ is perceptually similar to original image i.

$$E_e(i, w) \simeq i.$$

↓ embedding key e.

all watermarking schemes may not require e. only keyed embedding algos.

Blindness.

A watermarking scheme is called blind or oblivious if both D(.) and X(.) are

↓ detection algo

↓ extraction algo

Camlin Page
Date / /

independent of original image i and watermark w.

Formally, for all images i_1 and i_2 and watermarks w_1 and w_2 hold both

$$D_d(\bar{i}, i_1, w_1) = D_d(\bar{i}, i_2, w_2) \quad \text{— ①}$$

detection key

$$X_x(\bar{i}, i_1, \tilde{w}_1) = X(\bar{i}, i_2, \tilde{w}_2) \quad \text{— ②}$$

extraction key.

same O/P even when (i_1, w_1) and (i_2, w_2) changes → i and w not helping in D.

Similary, same O/P by $X(\cdot)$ even when i_1 and i_2 are different.

Invertibility

A watermarking scheme is invertible, reversible, lossless. if inverse of $E(\cdot)$ is computationally feasible.] ds the feasible to compute] computation in polynomial time ← not exponential

Also, it is used in $D(\cdot)$ to estimate the original image i from respective watermarked image $\bar{i}$.
Otherwise it is called non-invertible watermarking scheme.

original image can be extracted from $\bar{i}$ — invertible.

Camlin Page
Date / /

independent of original image i and watermark w.

Formally, for all images i_1 and i_2 and watermarks w_1 and w_2 hold both

$$D_d(\bar{i}, i_1, w_1) = D_d(\bar{i}, i_2, w_2) \quad \text{— ①}$$

detection key

$$X_x(\bar{i}, i_1, \tilde{w_1}) = X(\bar{i}, i_2, \tilde{w_2}) \quad \text{— ②}$$

extraction key.

same O/P even when (i_1, w_1) and (i_2, w_2) changes → i and w not helping in D.

Similary, same O/P by $X(\cdot)$ even when i_1 and i_2 are different.

Invertibility

A watermarking scheme is invertible, reversible, lossless. if inverse of $E(\cdot)$ is computationally feasible.] ds the feasible to compute] computation in polynomial not exponential ← time.

Also, it is used in $D(\cdot)$ to estimate the original image i from respective watermarked image $\bar{i}$.

Otherwise it is called non-invertible watermarking scheme.

original image can be extracted from $\bar{i}$ — invertible.

if $E_e(i, w) = \bar{i}$

then $E_e^{-1}(\bar{i}) = (i, w)$ exists

↓

Invertible

Semi blind

either detection is independent and extraction is not or vice versa.

— semi blind.

Non-blind

both extraction and detection algorithm need original image and watermark.

Robustness

Processed Image.

An image which is not essentially perceptually similar to original, but a certain amount of distortion δ is incurred by processing technique $p \in P$. — processed image.

If any image $I \in I$ is processed by p then for $p(I)$, following is true.

↓

processed image.

δ : quantify change.

$f(I) = I + \delta$.

applicable processing techniques for an application — P.

Eg: DCT, cropping etc.

A watermarking scheme is defined into following levels of robustness :

1) robust : if $D_d(f(\tilde{i}), i, w) = \tilde{i}, \tilde{w}$ $\forall f \in P$.

$\tilde{i}$ - estimated image data

$\tilde{w}$ - estimated watermark data.

2) fragile : if $D_d(f(\tilde{i}), i, w) = \perp$ (bot). $\forall f \in P$.

$\perp$ represents failure

3) semi fragile : if $D_d(f(\tilde{i}), i, w) = \tilde{i}, \tilde{w}$ $\forall f \in P_1$.

where $P_1 \subset P$.

$D_d(f(\tilde{i}), i, w) = \perp$ $\forall f \in (P - P_1)$

where $P_1 \subset P$.

$(P - P_1)$ does not belong to P_1.

δ : quantify change

$f(I) = I + \delta$.

applicable processing techniques for an application — P.

Eg: DCT, cropping etc.

A watermarking scheme is defined into following levels of robustness :

1) robust : if $D_d(f(\bar{i}), i, w) = \tilde{i}, \tilde{w}$ $\forall f \in P$.

$\tilde{i}$ - estimated image data

$\tilde{w}$ - estimated watermark data.

2) fragile : if $D_d(f(\bar{i}), i, w) = \downarrow$ (bot). $\forall f \in P$.

$\downarrow$ represents failure

3) semi fragile : if $D_d(f(\bar{i}), i, w) = \tilde{i}, \tilde{w}$ $\forall f \in P_1$.

where $P_1 \subset P$.

$D_d(f(\bar{i}), i, w) = \perp$ $\forall f \in (P - P_1)$

where $P_1 \subset P$.

$\downarrow$ does not belong to P_1.

15/3/19.

Embedding Capacity

watermarking embedding capacity for an image i is the max^m size of any watermark $w = G_g(i, m, j)$ for all m and j to be embedded in i such that $E_e(i, w) \approx i$, $D_d(E_e(i,w), i, w) = (\bar{i}, \bar{w})$ and there exists $\tilde{m}, \tilde{j} \mid \tilde{j} \approx j$ such that $X_x(E_e(i,w), i, \tilde{w}) = (\tilde{m}, \tilde{j})$

Error probability

A watermarking detection in a normal condition is said to be false positive if $D_d(i, w) \neq \perp$ for some i.

Conversely, if $D_d(\bar{i}, i, w) = \perp$ for some $\bar{i}$, watermark detection is false negative.

$D_d(i', i, w) \neq \perp, \quad i' \neq \tilde{i}$

i' - original o/p for embedding algorithm.

Security

A wat
secure
agains
hard
adversa

Elimino

Input

Output

Win condition

i_a is

Collusio

Input
cover image i
is same.

Output

Win cond

Maskin

A watermarking scheme is called A-secure if scheme retains the security against the attack A (i.e if it is hard to succeed with the set of adversary actions).

Elimination Attack

Input : Watermarked image $\bar{i}^{\circ} = E_e(i, w_0)$ where $w_0 \in W$

Output : attacked image $i_a \in \bar{I}$ such that $i_a \approx \bar{I}$ ($\tilde{i}$ (estimated))

Win condition : $D_d(i_a, i, w) = \perp$ for all w.

i_a is perceptually similar to $\bar{i}$.

Collusion Attack

Input : n copies of watermarked image cover image i is same. $\bar{I}_j = E_e(i, w_j)$, where $j = \{1, \ldots, n\}$ $(n \geq 2)$

Output : $i_a \in \tilde{i}$ such that $i_a \approx \bar{i}_j$.

Win condition : $D_d(i_a, i, w) = 1 \ \forall w$.

Masking attack

Input : A watermarked image $\bar{i} = E_e(i, w_0)$ where $w_0 \in W$.

Output : $i_a \in \bar{I}$ such that $i_a \approx \bar{i}$

Win cond^n : $D_d(i_a, i, w_0) = 1$ but there exists $w \neq w_0$ such that $D_d(i_a, i, w) \neq 1$.

Distortion attack — degrade $\bar{i}$ by applying processing technique.

Input : A watermarked image $\bar{i} = E_e(i, w_0)$ and processing technique $q \in Q$ where Q is set of applicable processing techniques such that $Q \subseteq IP$.

Output : processed image $q(\bar{i})$.

Win condition : $D_d(q(\bar{i}), i, w_0) = 1$ but there exists $w \neq w_0$ such that $D_d(q(\bar{i}), i, w) \neq 1$.

Forgery attack — (generate invalid watermark image so that it passes)

Input : A new unwatermarked image i_a $i_a \in I$, a new watermark $w_a \in W$ and access to $E_e(\cdot)$.

Output : A new watermarked image $\bar{i}_a$.

w/o knowing embedding key.

Win condition : $D_d(\bar{I}_a, i_a, w_a) \neq 1$
there exists $w_a \in W$ such that ↑.

Copy attack

Input : A valid watermarked image $\bar{i} = E_e(i, w_o)$, a new unwatermarked image $i_a \in I$ and access to $E_e(\cdot)$.

Output : new watermarked image $\bar{i}_a = E_e(i_a, \tilde{w}_o)$
↳ from watermarked image.

Win condition : There exists $\tilde{w}_o \in W$.
such that $D_d(\bar{i}_a, i_a, \tilde{w}_o) \neq 1$ where $\tilde{w}_o$ is estimate of w_o.

forgery attacks more difficult → less I/P.
than copy attacks → more I/P

Ambiguity attack (double watermark on 1 image)

Input : valid watermarked image $\bar{i} = E_e(i, w)$ and access to $E(\cdot)$.

Output : new watermarked image $\bar{i}_a = E_e(\bar{i}, w_a)$.

Win condition : There exists $w_a \in W$ such that $D_d(\bar{i}_a, I, w_a) \neq 1$.

Scrambling attack.

Input : A watermarked image $\bar{i} = E_e(i, w_0)$ where $w_0 \in W$ and access to suitable scrambling and descrambling functions.

Output : An image $\bar{i}_a \in \bar{i}$ from scrambling samples of $\bar{i} \in \bar{I}$ (before detection, and descrambles back to $\bar{i} \in \bar{I}$ after detection)

$D_d(\bar{i}_a, i, w_0) = 1$ but there exists $w \neq w_0$ such that $D_d(\bar{i}_a, i, w) \neq \perp$.

Passive attack

not modifying watermark image.

level 1 (detection only)

visible/ invisible wm

an adversary only detects the presence of valid watermark $w \in W$ in a watermarked image $\bar{i} \in \bar{I}$

level 2 (Incisive detection)

adversary distinguishes watermark w

level 2 - level 1 ✓
level 2 ✓ .

Camlin | Page
Date / /

from that of other watermarked image (s). $\bar{I} \in \bar{I} \mid \bar{I} \neq \bar{i}$.

level 3 (comperehensive detection).

adversary gets partial info (m, j) that $w \in W$ carries without modifying $\bar{i}$.

$m \in M$, $j \in J$, $\bar{I} \in \bar{I}$, $w \in W$.

level 3 succeeds ⇒ level 1 and level 2 also succeeds.

Similarity and differences b/w attacks.

I/P - challanger of W/M scheme is giving I/P.