數位影像的保護與驗證技術

Protection and Authentication of Digital Image

演講者：林志鴻（多媒體資訊與安全實驗室）

服務單位：南台科技大學 資訊工程系

演講地點/日期：國立屏東商業技術學院資科所/ 2007.10.28

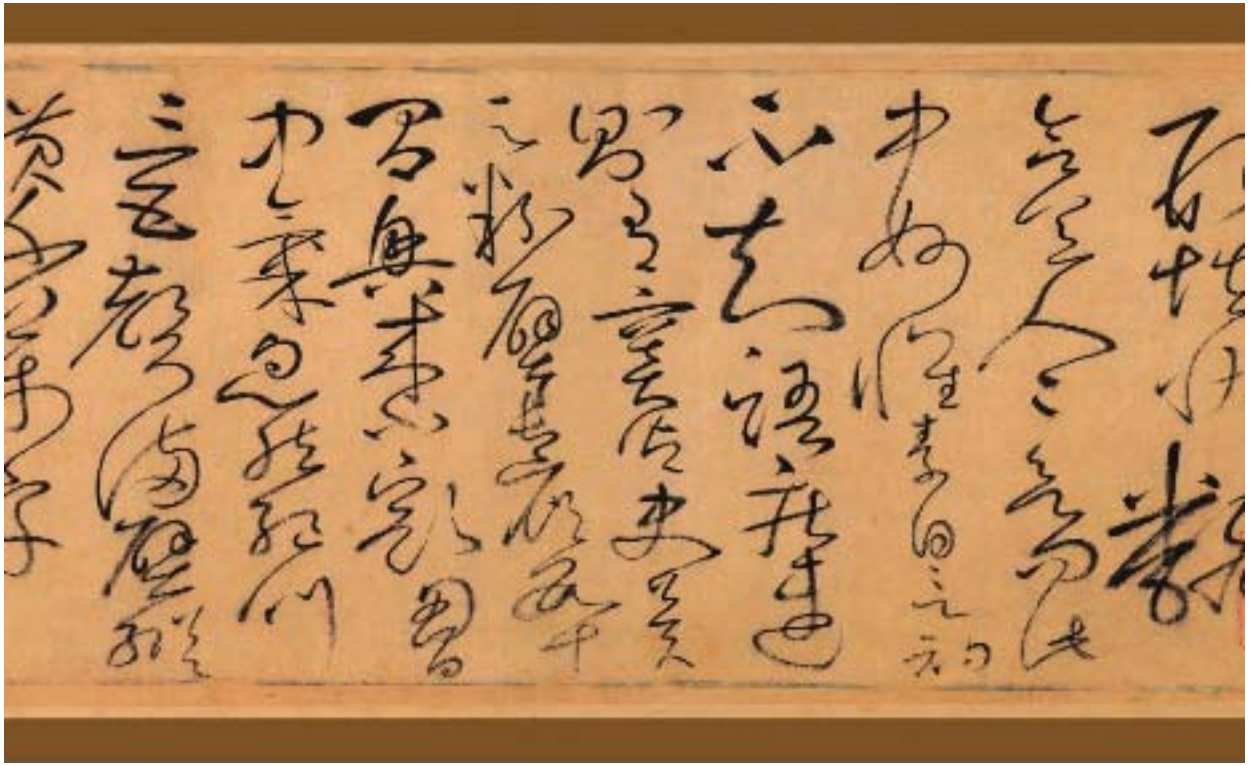
我的傳家之寶


國立故宮博物院
NATIONAL PALACE MUSEUM
新裝飾的時代
—明代前期的官營作坊
The New Era of Ornamentation: 1350-1521
國立故宮博物院版權所有 Copyright© National Palace Museum. All Rights Reserved.

猜猜看　這是誰的作品?

晉　王羲之
平安何如奉橘三帖
卷　紙本　縱：24.7公分　橫：46.8公分

我國中時期的書法課作品



唐　懷素
自敘帖
卷　紙本　縱：28.3公分　橫：755公分

懷素（約活動於八世紀三十年代至七十年代）本姓錢，字藏真，僧名懷素。生於湖南零陵縣，後來移居長沙。

誰是原著者?

誰是擁有者?

大家來找碴！

哪裡被修改?

哪裡被僞造?

大家來找碴 II

原始影像

壓縮影像

如何分辨
善意與惡意?

- **Copyright Protection**
  - Robust
- **Integrity Verification**
  - Fragile

- **Malicious / Non-malicious modification**
  - Semi-fragile

Outline

1. Introduction
   - 1. background
   - 2. related works
   - 3. motivation
2. Applying Vector Projection to Fragile Image Authentication
3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images
4. Semi-Fragile Watermarking Scheme for Authentication of JPEG Images

Outline

5 **Image Authentication Scheme for Resisting the JPEG, JPEG2000 Compression and Scaling**

6 **Conclusions and Future Works**

1. Introduction- Background

- secr
- auth
- inte
- non- on

sender

attack

hacker

receiver

1. Introduction- Background

Methods

Protection and Authentication of Digital Image

Digital Watermark-based

embed ← **watermark**

=

watermarked image

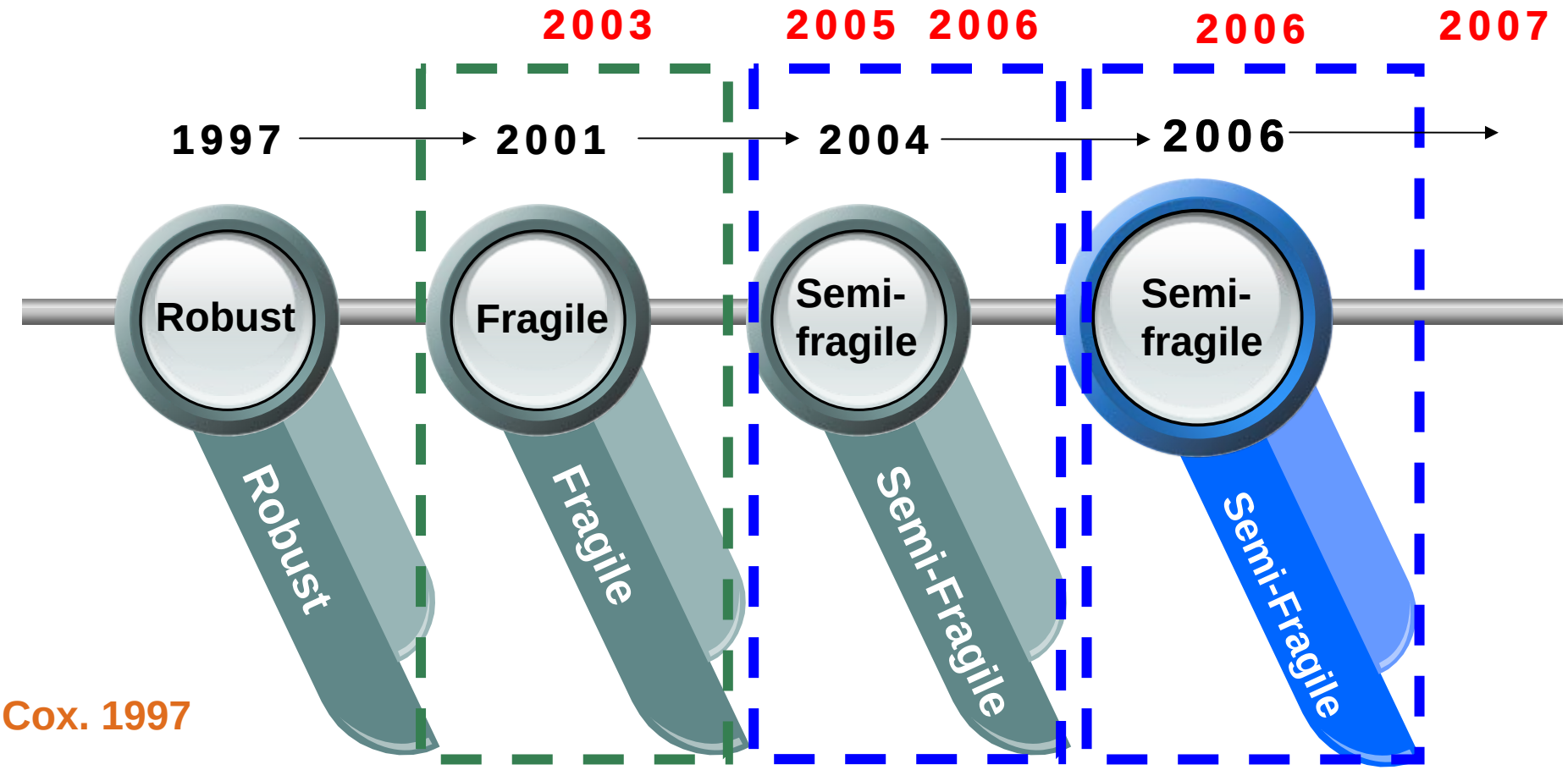
- ***invisible***
- ***universality***
- ***unambiguousness***

Digital Signature-based

+ signature

- ***Secret-key cryptosystem***
  - DES
- ***Public-key cryptosystem***
  - RSA,DSA
- ***Hash***
  - MD5

1. Introduction- Background



Cox. 1997

Copyright protection

Ownership verification

Withstand nearly all attacks

Content authentication

Integrity verification

Fragile to almost all manipulations

Robust to non-malicious manipulations

1. Introduction- Related works

Fragile image authentication:

- P. W. Wong and N. Memon [Wong 1998] proposed a watermark-based image authentication method based on block-wise
- M. Holliman and N. Memon [Holliman 2000] presented a class of attacks on block-wise watermark schemes – VQ attack
- Celik, Sharma, Saber and Tekalp [Celik 2002] provided a solution, which using the hierarchical structure, that thwarts the VQ attack

1. Introduction- Related works

- **Semi-fragile image authentication:**
  - ***vector quantization (VQ)***
    - [Lu 2003] (spatial, watermark-based)
  - ***singular value decomposition (SVD)***
    - [Sun, R. 2002] (spatial, watermark-based)
    - [Bao 2005] (wavelet, watermark-based)
  - ***error correction coding (ECC)***
    - [Zhou 2004] (spatial/wavelet_LL)
  - ***mathematical morphology***
    - [El-Din 2002] (spatial, signature-based)
    - [Wu 2004] (DCT, watermark-based)
    - [Schneider 1996] (histogram maps, edge/corner maps)
- **Achieved purposes:**
  - robust to JPEG compression (non-malicious manipulation)
  - locate manipulated positions

1. Introduction- Related works

- **Non-malicious v.s. malicious manipulations**
  - blurring manipulation
    - *non-malicious:*
      - [Hu Y-P 2005] [Feng 2005]
    - *malicious:*
      - [Sun, Q. 2005] [Schneider 1996] [Lin 2001] [Lu C.-S. 2003] [Venkatesan 2000]
  - adding noise, rotation, sharpening and lowpass/highpass filtering, also present ambiguous cases

1. Introduction- Motivation

- **Fragile image authentication**
  - thwart the counterfeit attack
  - present the solid analysis
- **Semi-fragile image authentication**
  - the lower bound sensitivity of fragility can be determined
  - present the solid analysis

1. Introduction- Motivation

Semi-fragile image authentication

- non-malicious manipulation is clearly defined
- only the spatial domain is adopted during feature generation and verification
- more non-malicious manipulated images (JPEG, JPEG2000 compressed and scaled images) can be authenticated

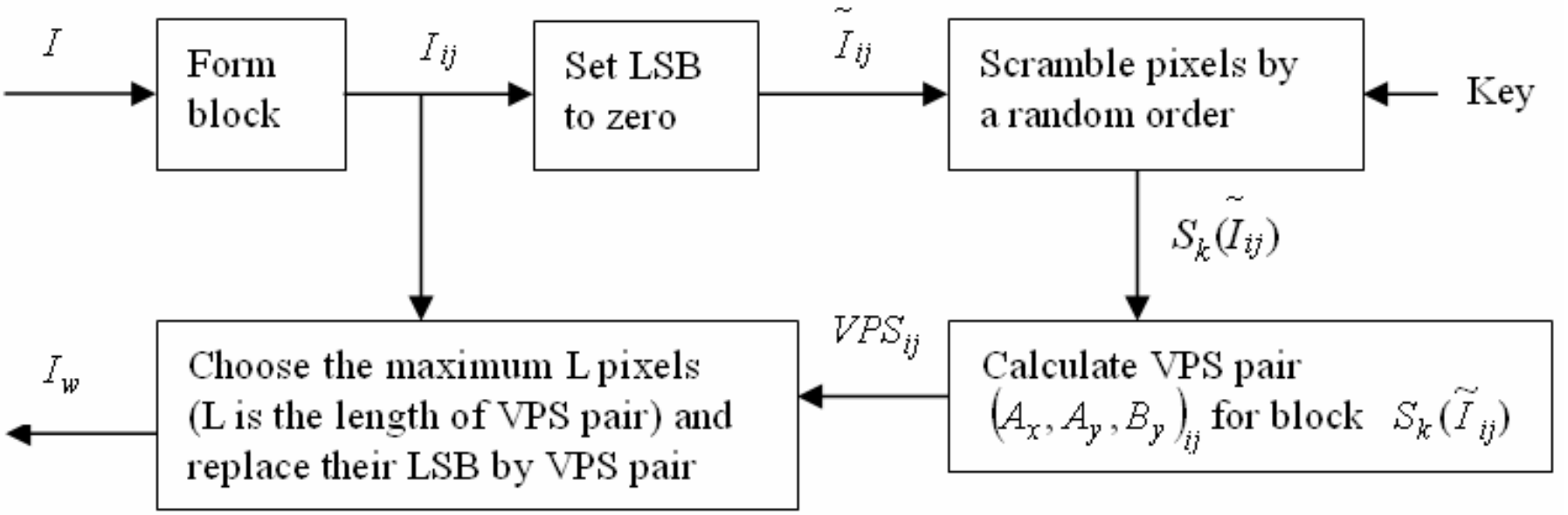
Outline

1. Introduction
2. Applying Vector Projection to Fragile Image Authentication
3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images
4. Semi-Fragile Watermarking Scheme for Authentication of JPEG Images

2. Applying Vector Projection to Fragile Image Authentication

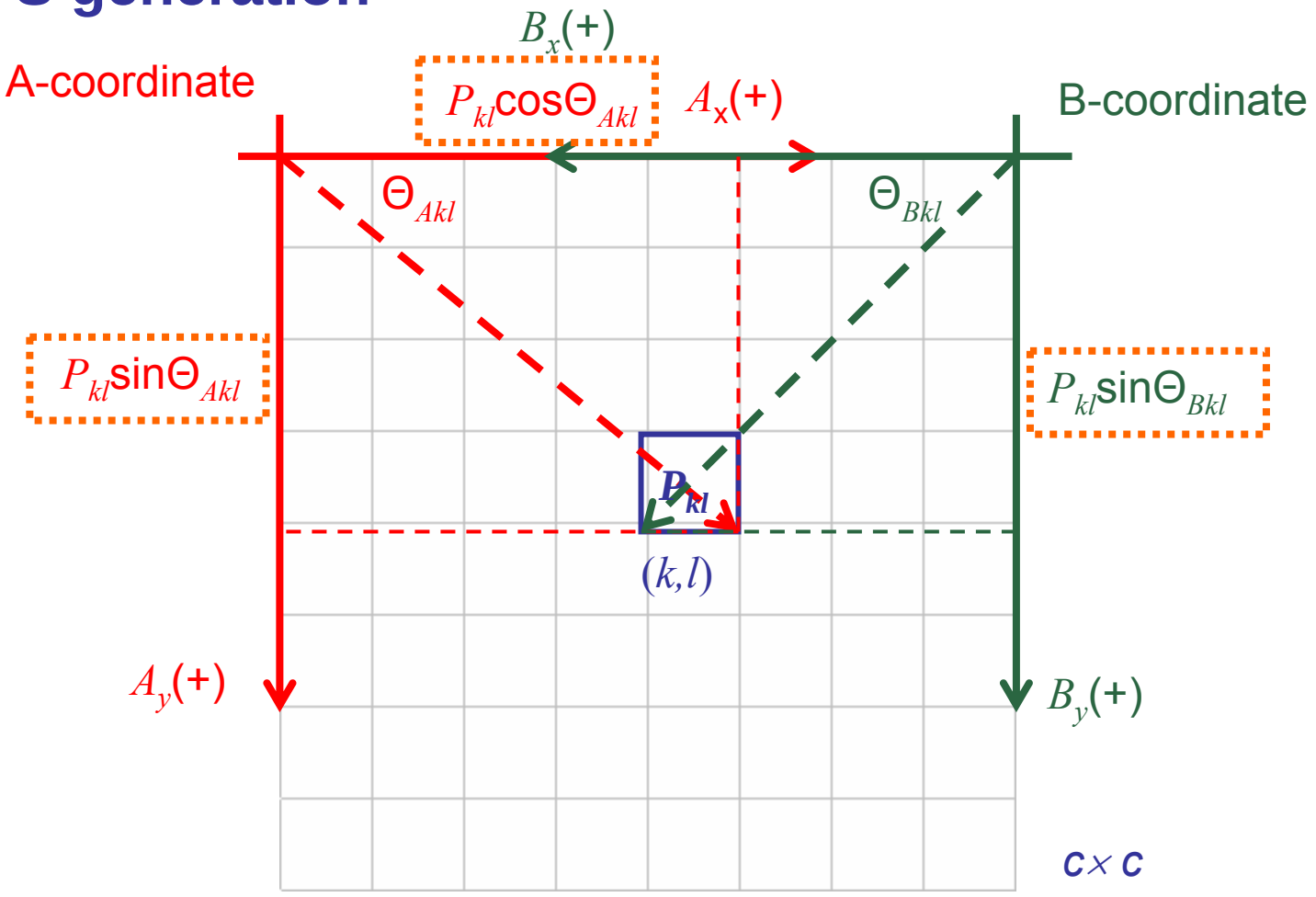
- The Vector Projective Square (VPS) pair of each block can be calculated by a vector projection technique
- Four goals:
  - (1) verify authentication
  - (2) verify integrity
  - (3) locate parts that were illegally modified or counterfeited
  - (4) provide security against counterfeit attacks

2. Applying Vector Projection to Fragile Image Authentication



VPS generation and insertion process

A. VPS generation



Relationship between P_{kl} , A-coordinate and B-coordinate. $c \times c$ is the block size

2. Applying Vector Projection to Fragile Image Authentication

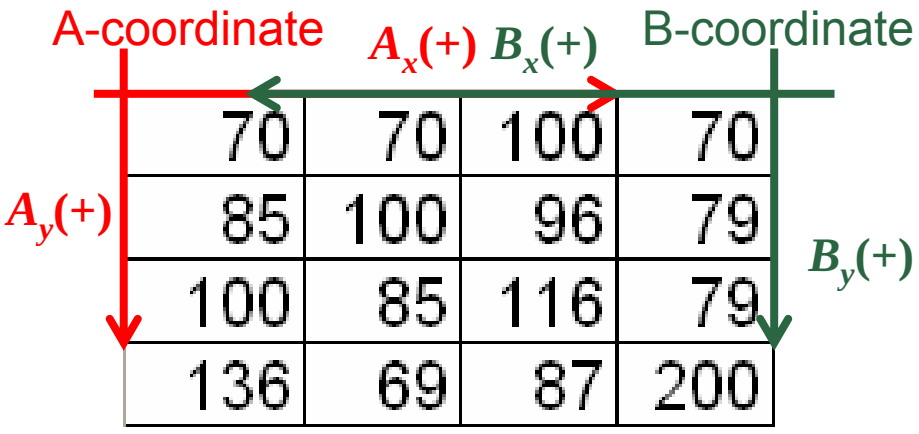
$$A_x = \sum_{k=0}^{c-1}\sum_{l=0}^{c-1}\left(P_{kl}\cdot\cos\theta_{Akl}\right)^2$$

$$A_y = \sum_{k=0}^{c-1}\sum_{l=0}^{c-1}\left(P_{kl}\cdot\sin\theta_{Akl}\right)^2$$

$$B_y = \sum_{k=0}^{c-1}\sum_{l=0}^{c-1}\left(P_{kl}\cdot\sin\theta_{Bkl}\right)^2$$

$$\text{VPS pair} = \left(A_x, A_y, B_y\right)_{ij}$$

Example : block size is 4×4



VPS pair

$$A_x = \sum_{k=0}^{4-1}\sum_{l=0}^{4-1}\left(P_{kl}\cdot\cos\theta_{Akl}\right)^2 = 21753$$

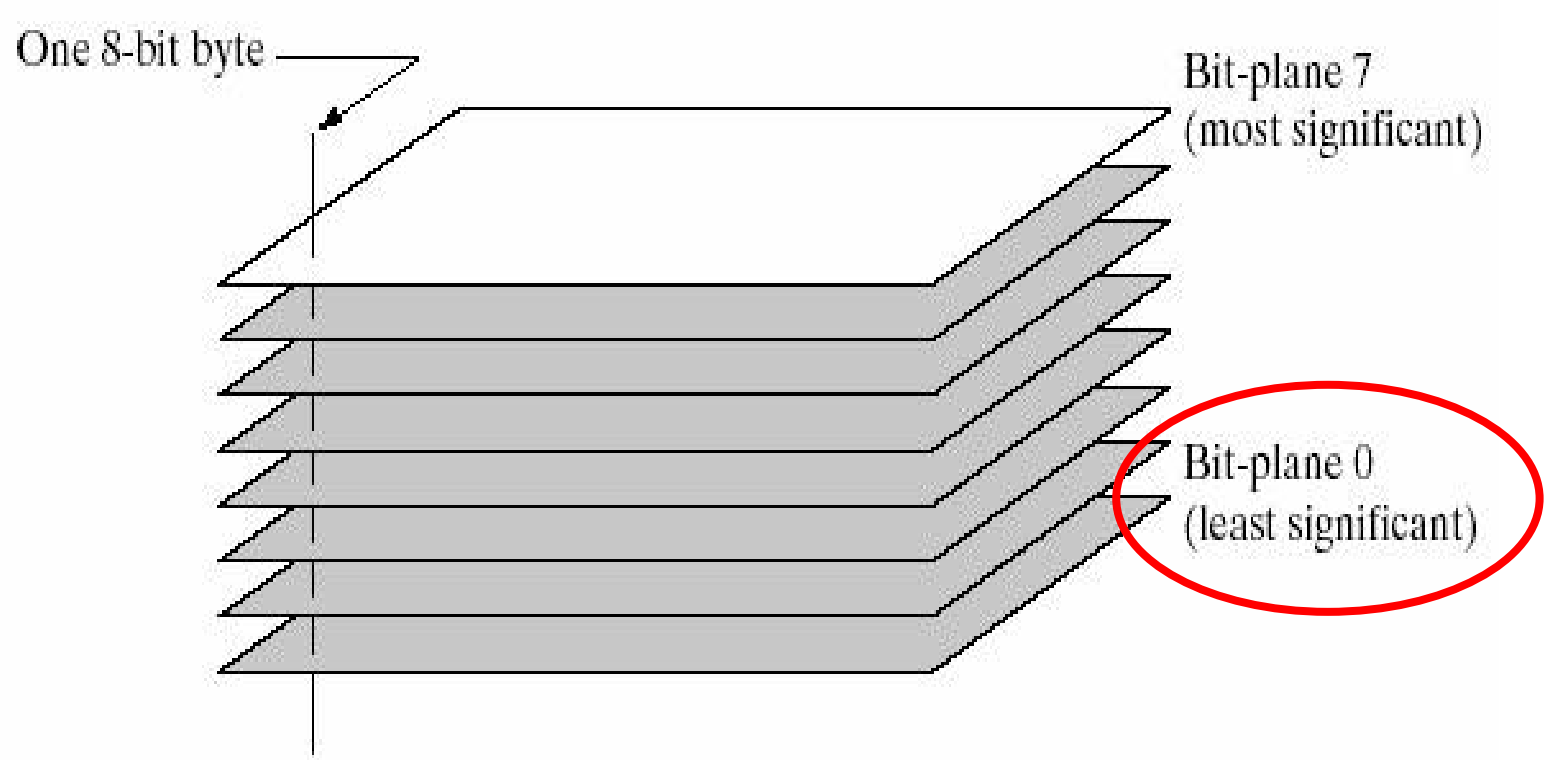
$$A_y = \sum_{k=0}^{4-1}\sum_{l=0}^{4-1}\left(P_{kl}\cdot\cos\theta_{Akl}\right)^2 = 19289$$

$$B_y = \sum_{k=0}^{4-1}\sum_{l=0}^{4-1}\left(P_{kl}\cdot\cos\theta_{Akl}\right)^2 = 20695$$

→ VPS pair
$= (21753,19289,20695)_{10}$
$= (1010\ldots111)_2$, 45bits

2. Applying Vector Projection to Fragile Image Authentication

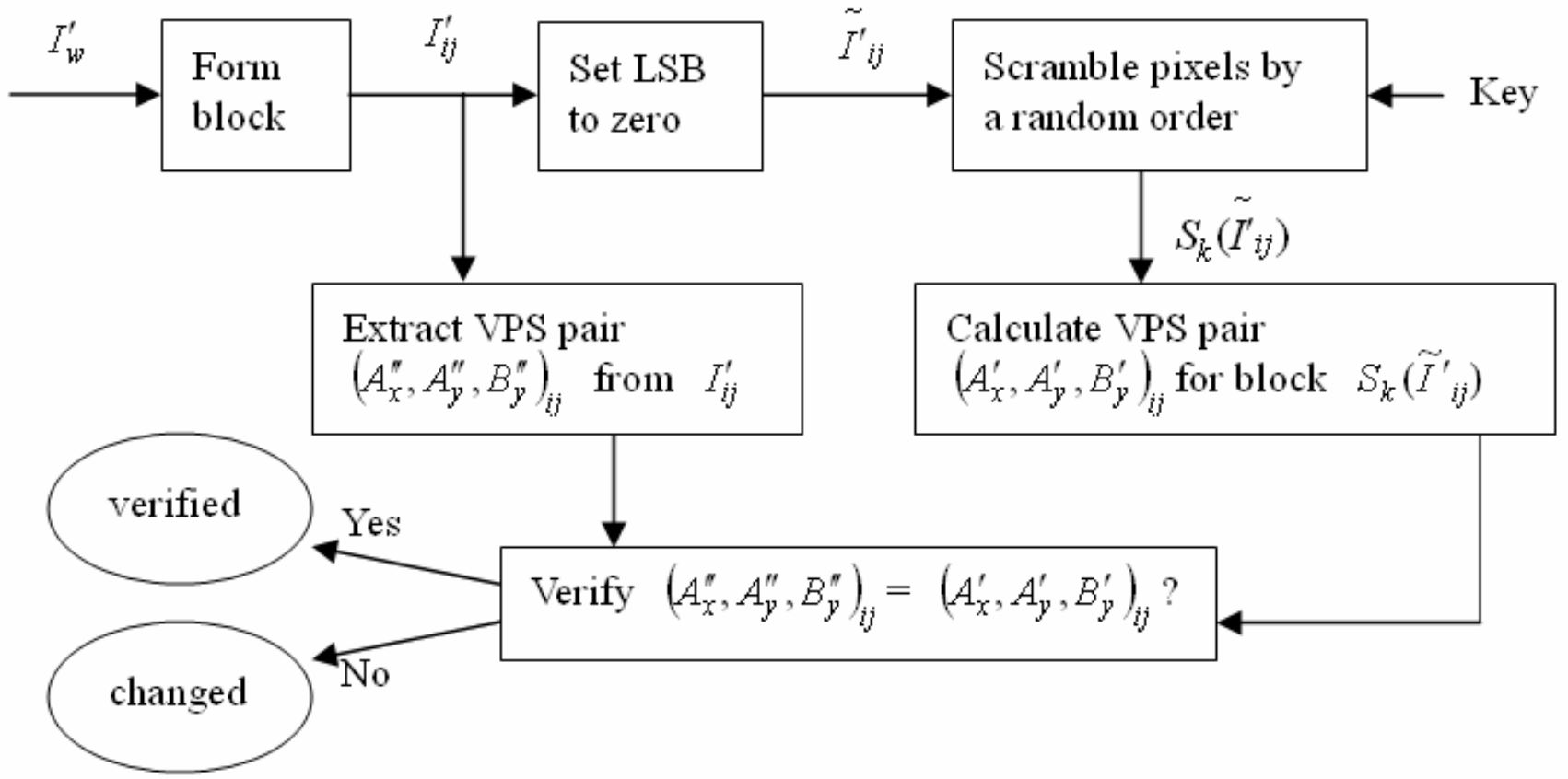
- insert watermark into the bit-plane 0



8 bit-planes of an image

2. Applying Vector Projection to Fragile Image Authentication

B. integrity verification



Integrity verification process for the proposed method

2. Applying Vector Projection to Fragile Image Authentication

Visual quality of watermarked image

- for example, let $c=2^3$ and $0 \le P_{kl} < 2^8$, in 8×8 block, we can embed a 60 (=3 ×[2 ×(3-1)+2 ×8])bits VPS pair, and the average modified pixels are only 30, the modified value may be +1 or -1, so it is easy to calculate that the ***Peak Signal to Noise Ratio*** (PSNR) of the watermarked image is about

$$10 \times \log\left(255^2 \Big/ \left(30 \times 1/64\right) \right) = 51.4 \text{ dB}$$

2. Applying Vector Projection to Fragile Image Authentication

Analysis

- **Assumption:** an attempt has been made to create a counterfeit image I' that has the same VPS pairs $(A'_x, A'_y, B'_y)_{ij}$ as the VPS pairs $(A_x, A_y, B_y)_{ij}$ of the original image I for all blocks, this means that $(A'_x, A'_y, B'_y)_{ij} = (A_x, A_y, B_y)_{ij}$ for all I_{ij} blocks.

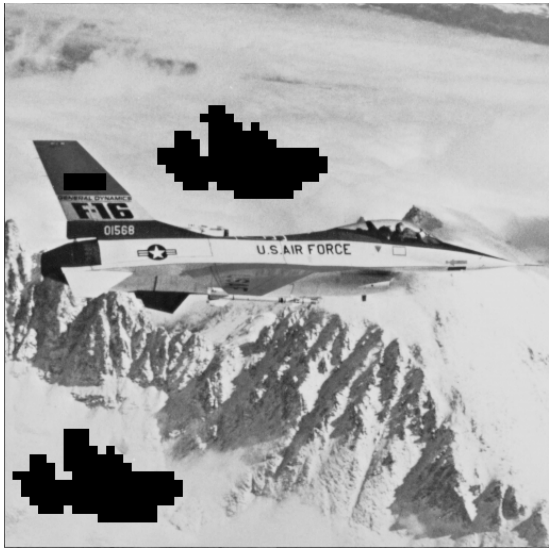
$$(A_x, A_y, B_y)_{ij} \neq (A'_x, A'_y, B'_y)_{ij}$$

2. Applying Vector Projection to Fragile Image Authentication

❖ Experimental result:

(a)

(b)



(c)

(a) original image (512×512 pixels), (b) altered image, (c) detection output.

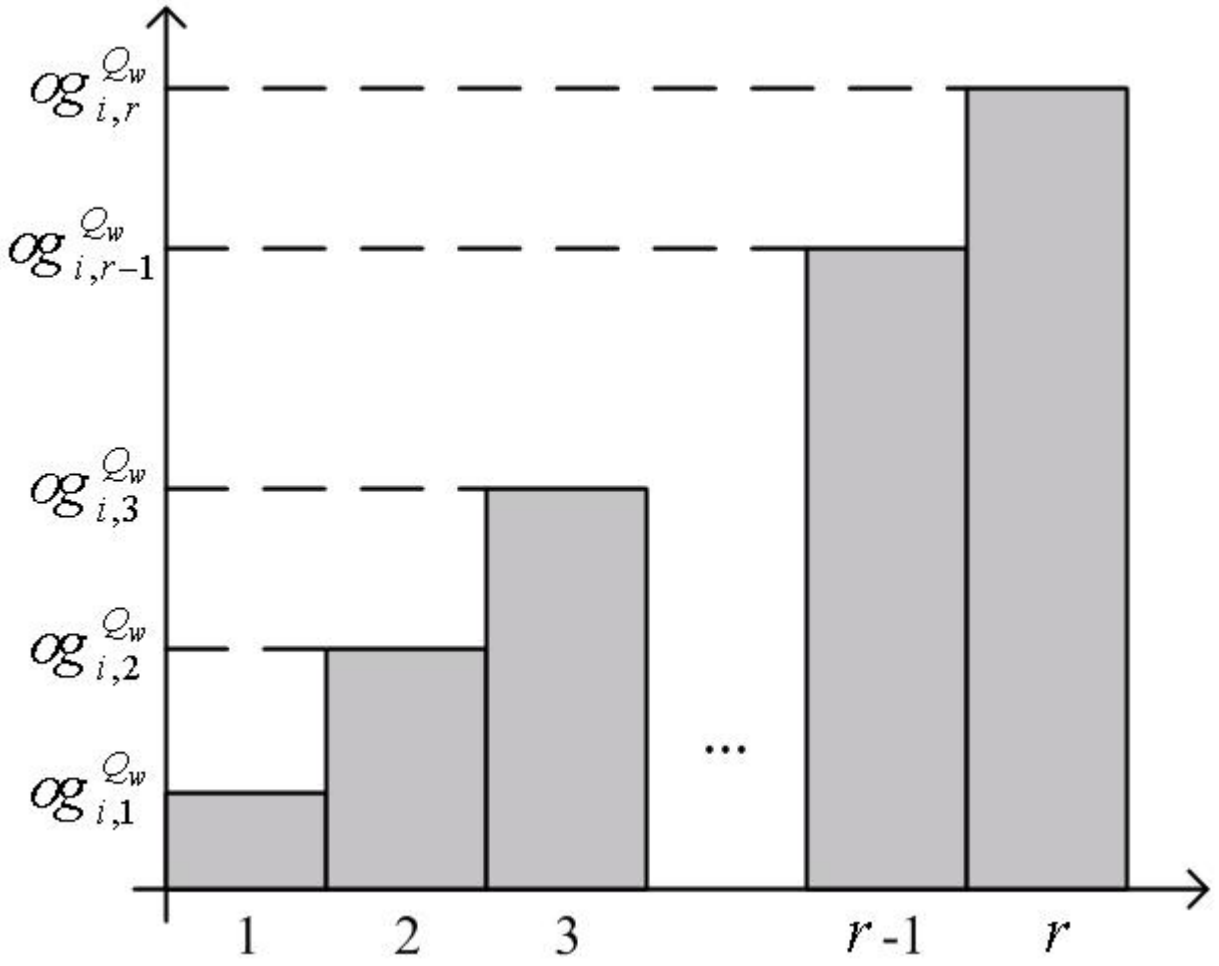
Outline

1. Introduction
2. Applying Vector Projection to Fragile Image Authentication
3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images
4. Semi-Fragile Watermarking Scheme for Authentication of JPEG Images

3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images

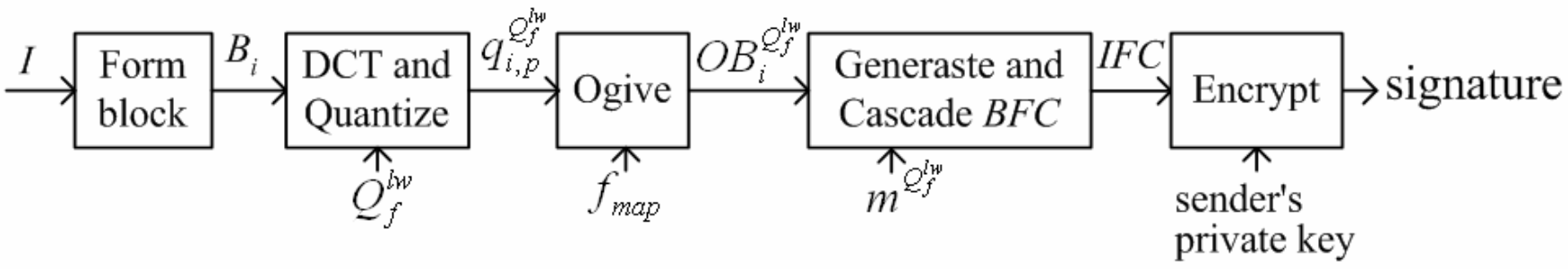
- Adopt statistic Ogive analysis in quantized discrete cosine transform (*DCT*) coefficients to construct a feature code
- The degree of fragility can be easily adjusted by simply controlling a fragile degree factor (*FDF*)
- Analyze how to choose *FDF* and the critical image feature properties

3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images

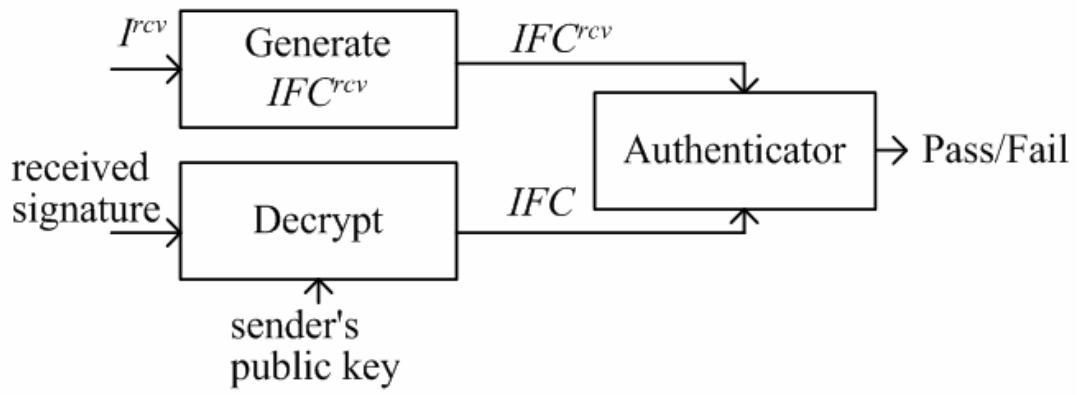


The Ogive graph ($OG_i^{Q_w}$) with lower bound JPEG quality factor

3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images



(a)



(b)

(a) block diagram of the proposed image feature code generator, (b) block diagram of the image authentication

3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images

❖ Example:

70	70	100	70	87	87	150	187
85	100	96	79	87	154	87	113
100	85	116	79	70	87	86	196
136	69	87	200	79	71	117	96
161	70	87	200	103	71	96	113
161	123	147	133	113	113	85	161
146	147	175	100	103	103	163	187
156	146	189	70	113	161	163	197

pixels in block

DCT →

-80	-40	89	-73	44	32	53	-3
-135	-59	-26	6	14	-3	-13	-28
47	-76	66	-3	-108	-78	33	59
-2	10	-18	0	33	11	-21	1
-1	-9	-22	8	32	65	-36	-1
5	-20	28	-46	3	24	-30	24
6	-20	37	-28	12	-35	33	17
-5	-23	33	-30	17	-5	-4	20

DCT coefficients

quantize ↓

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

quantization table

→

-5	-4	9	-5	2	1	1	0
-11	-5	-2	0	1	0	0	1
3	-6	4	0	-3	-1	0	1
0	1	-1	0	1	0	0	0
0	0	-1	0	0	1	0	0
0	-1	1	-1	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

quantized DCT coefficients

3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images

(-3, 9, -1, -11, 4)

↓ absolute

(3, 9, 1, 11, 4)

↓ form Ogive graph

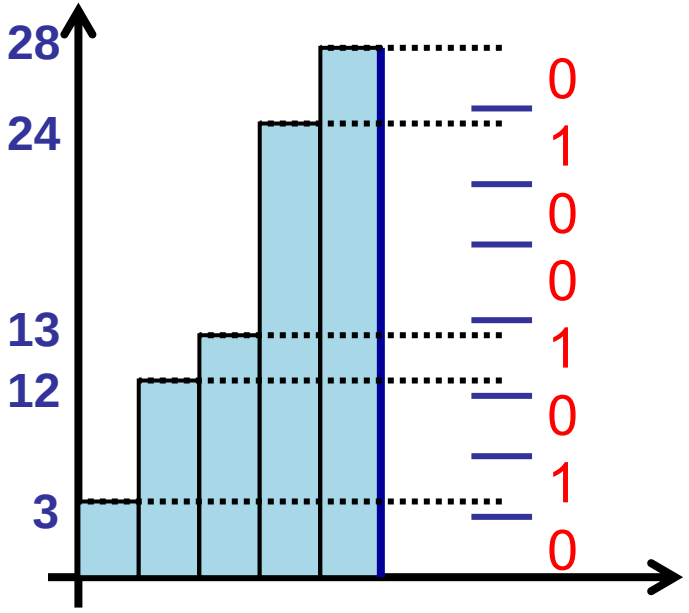


image feature code

- block feature code (BFC_i) = $(01010010)_2$
- image feature code (IFC) =

$$IFC = \bigcup_{i=1}^{M \times N / b^2} BFC_i$$

Analysis and discussion

- ***Discussion A***: How can *FDF* m^{Qw} be chosen, such that the proposed method is robust to the lower bound of the sensitivity of fragility corresponding to JPEG compression with quality factor Q, where $Q \geq Q_w$?
- ***Lemma A***: The Ogive image feature is robust to JPEG compression with quality factor Q, where $Q \geq Q_w$.
- ***Lemma B***: The Ogive image feature is fragile to other attacks other than JPEG compression with quality factor Q, where $Q \geq Q_w$, making the image be forged difficultly.

3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images

❖ Experimental results

Barbara

Boat

Goldhill

Lena

- image size: 512×512 pixels
- block size: 8×8 pixels
- 10 quantized DCT coefficients were selected to form the Ogive graph

3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images

The relationship between the lower bound of the JPEG quality factor Q_w, fragile degree factor m^{Qw} and the compression rate ***CR*** (*CR* = original file size : compressed file size) for each image. (Q_w is set from 30 to 90).

Q_w		Barbara	Boat	Goldhill	Lena
30	m^{30}	3	3	3	3
	CR	32:1	37:1	37:1	48:1
40	m^{40}	4	4	4	4
	CR	27:1	31:1	31:1	41:1
50	m^{50}	6	6	6	7
	CR	24:1	28:1	27:1	37:1
60	m^{60}	8	7	7	8
	CR	21:1	24:1	23:1	32:1
70	m^{70}	10	9	10	11
	CR	18:1	20:1	20:1	27:1
80	m^{80}	19	18	16	18
	CR	15:1	15:1	16:1	21:1
90	m^{90}	22	21	20	21
	CR	10:1	10:1	10:1	14:1

JPEG QF	30	40	50	60	70	80	90
PSNR (dB)	33.6~34.3	34.2~35.1	34.8~35.8	35.3~36.5	35.9~37.3	36.8~38.5	38.8~41.2

3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images

Authentication results for several attacks. (Q_w is set to 50).

Attacks	Barbara	Boat	Goldhill	Lena
Cropping	*F*	*F*	*F*	*F*
Pasting	*F*	*F*	*F*	*F*
Rotation	*F*	*F*	*F*	*F*
JPEG Quality = 40	*F*	*F*	*F*	*F*
JPEG Quality ≥ 50	*P*	*P*	*P*	*P*
Gaussian noise	*F*	*F*	*F*	*F*
Gaussian filter	*F*	*F*	*F*	*F*
Median filter	*F*	*F*	*F*	*F*
Histogram equalization	*F*	*F*	*F*	*F*
Brightness	*F*	*F*	*F*	*F*
Contrast	*F*	*F*	*F*	*F*

3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images

(a) (b) (c)

Malicious manipulation attacks (a) The original Goldhill image, (b) The manipulated image, (c) The authentication result image.

3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images

Compare the proposed method with related semi-fragile methods in terms of four properties.

Abilities and Properties	Ogive	Lu 2003	SunR. 2002	Sun Q. 2002	Zhou 2004	El-Din 2002	Li 2004	Bao 2005	Lu 2005
Robust to JPEG compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Locate manipulations	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Adjust fragile degree	Yes	Yes	No	No	Yes	Yes	Yes	No	No
Analyzes and arguments about controlling sensitive of fragility	Yes	No	No	No	No	No	No	No	No
Set lower bound JPEG quality	Yes	No	No	No	No	No	Yes	No	No

Outline

1. Introduction
2. Applying Vector Projection to Fragile Image Authentication
3. Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images
4. Semi-Fragile Watermarking Scheme for Authentication of JPEG Images

4. Semi-Fragile Watermarking Scheme for Authentication of JPEG Images

- Presents a novel digital watermarking method for verifying the authentication of JPEG images, in terms of a unique concept named lowest authenticable JPEG quality (LAJQ)
- The image feature is generated from DCT coefficients where in low/middle frequency domain
- The image feature is embedded into the high frequency domain for protection

4. Semi-Fragile Watermarking Scheme for Authentication of JPEG Images

❖Example (feature generation)

70	70	100	70	87	87	150	187
85	100	96	79	87	154	87	113
100	85	116	79	70	87	86	196
136	69	87	200	79	71	117	96
161	70	87	200	103	71	96	113
161	123	147	133	113	113	85	161
146	147	175	100	103	103	163	187
156	146	189	70	113	161	163	197

pixels in block$_{25}$

DCT →

-80	-40	89	-73	44	32	53	-3
-135	-59	-26	6	14	-3	-13	-28
47	-76	66	-3	-108	-78	33	59
-2	10	-18	0	33	11	-21	1
-1	-9	-22	8	32	65	-36	-1
5	-20	28	-46	3	24	-30	24
6	-20	37	-28	12	-35	33	17
-5	-23	33	-30	17	-5	-4	20

DCT coefficients

quantize ↓

-5	-4	9	-5	2	1	1	0
-11	-5	-2	0	1	0	0	-1
3	-6	4	0	-3	-1	0	1
0	1	-1	0	1	0	0	0
0	0	-1	0	0	1	0	0
0	-1	1	-1	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

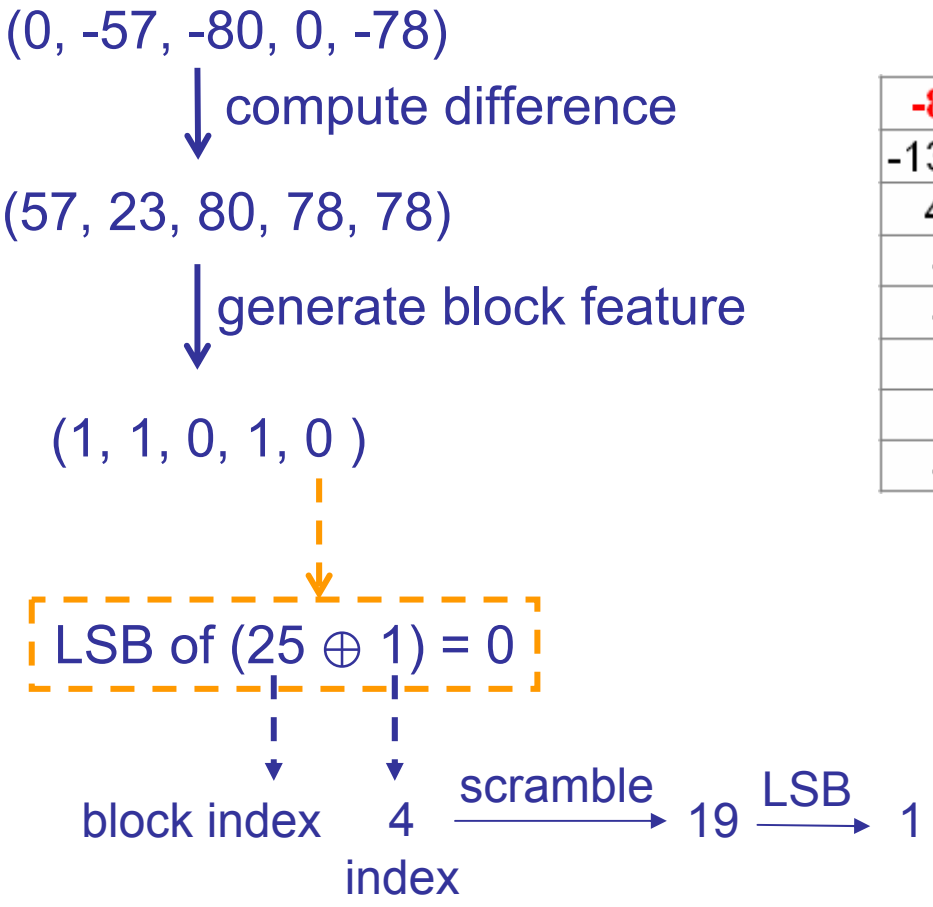
quantized DCT coefficients

de-quantize →

-80	-44	90	-80	48	40	51	0
-132	-60	-28	0	26	0	0	-55
42	-78	64	0	-120	-57	0	56
0	17	-22	0	51	0	0	0
0	0	-37	0	0	109	0	0
0	-35	55	-64	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

de-quantized DCT coefficients

4. Semi-Fragile Watermarking Scheme for Authentication of JPEG Images



-80	-40	89	-73	44	32	53	-3
-135	-59	-26	**0**	14	-3	-13	-28
47	**-78**	66	-3	-108	**-57**	33	59
-2	10	-18	0	33	11	-21	1
-1	**0**	-22	8	32	65	-36	-1
5	-20	28	-46	3	24	-30	24
6	-20	37	-28	12	-35	33	17
-5	-23	33	-30	17	-5	-4	20

modified DCT coefficients

4. Semi-Fragile Watermarking Scheme for Authentication of JPEG Images

❖Feature embedding

(-21, -5, 3, 33, 37) ← embed — (1, 1, 0, 1, 0)

- because | -21 | < 80 + (80/2)
  → -21 is modified to – [80 + (80/2)] = -120
- because |3| < 81/2
  → no change
- for embedding:
  (-21, -5, 3, 33, 37) → (-120, -108, 3, 180, 37)

-80	-40	89	-73	44	32	53	-3
-135	-59	-26	**0**	14	-3	-13	-28
47	**-78**	66	-3	-108	**-57**	33	59
-2	10	-18	0	33	11	**-120**	1
-1	**0**	-22	8	32	65	-36	-1
5	-20	28	-46	3	24	-30	24
6	-20	37	-28	12	-35	**180**	17
-108	-23	33	-30	17	-5	-4	20

DCT coefficients of watermarked block

-80	-40	89	-73	44	32	53	-3
-135	-59	-26	**0**	14	-3	-13	-28
47	**-78**	66	-3	-108	**-57**	33	59
-2	10	-18	0	33	11	-21	1
-1	**0**	-22	8	32	65	-36	-1
5	-20	28	-46	3	24	-30	24
6	-20	37	-28	12	-35	33	17
-5	-23	33	-30	17	-5	-4	20

modified DCT coefficients

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

quantization table

4. Semi-Fragile Watermarking Scheme for Authentication of JPEG Images

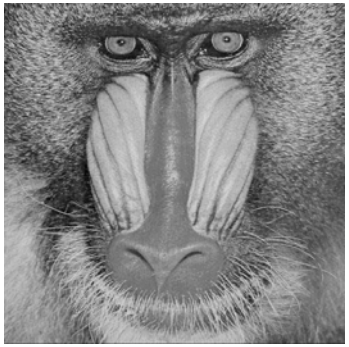
- **Analysis and discussion**
  - validity of image feature generation and authentication method
  - validity of image feature embedding method

4. Semi-Fragile Watermarking Scheme for Authentication of JPEG Images

❖ Experimental results

- image size: 512×512 pixels
- block size: 8×8 pixels
- five watermarked images:


Airplane


Baboon


Lena


Pepper


Car

The PSNR(dB) of watermarked images for the proposed method and related works.

	Airplane	Baboon	Lena	Pepper	Car
Proposed method	35.68	40.52	37.38	36.97	37.72
[Lu 2005]	25.43	21.35	26.64	25.95	25.11
[Li 2004]	32.72	26.87	33.12	32.60	30.40

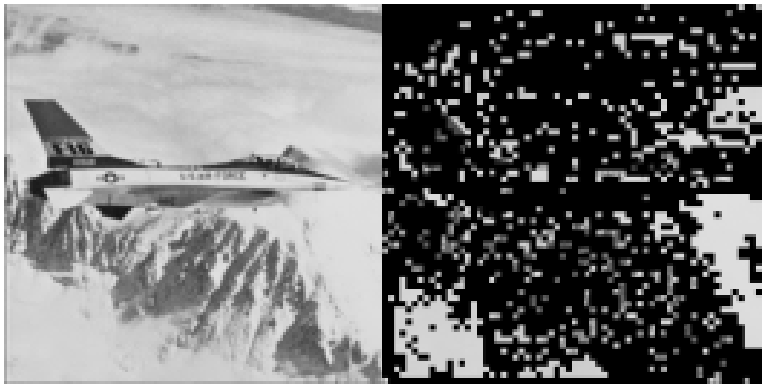
❖ *Experiment 1:*

- *Detection of blur, sharp, contrast (adjust histogram), Gaussian lowpass filter:*

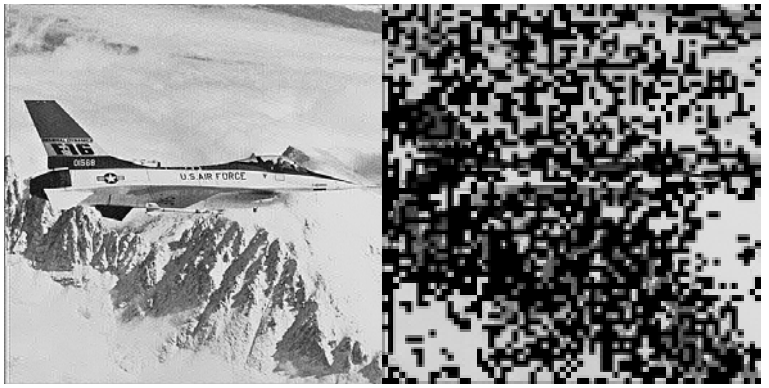
The masks or functions were used for blur, sharp, contrast (adjust histogram) and Gaussian lowpass filter attacks by MATLAB.

Attack	Blur	Sharp	Contrast (adjust histogram)	Gaussian Lowpass Filter
Mask or Function	$\begin{bmatrix} 0.1 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.1 \end{bmatrix}$	$\begin{bmatrix} -0.17 & -0.67 & -0.17 \\ -0.67 & 4.33 & -0.67 \\ -0.17 & -0.67 & -0.17 \end{bmatrix}$	Histeq Function	$\begin{bmatrix} 0.01 & 0.08 & 0.01 \\ 0.08 & 0.62 & 0.08 \\ 0.01 & 0.08 & 0.01 \end{bmatrix}$

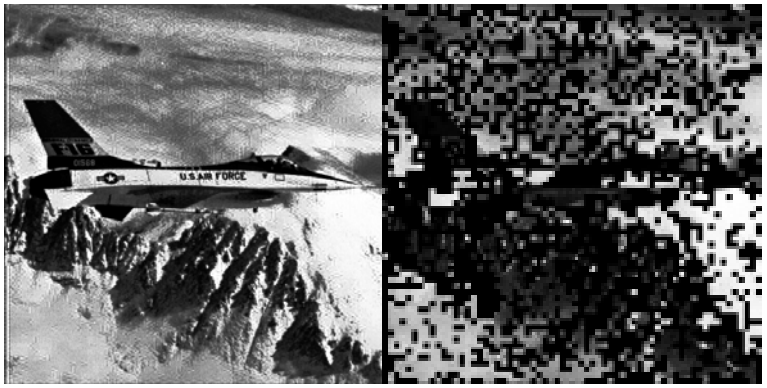
4. Semi-Fragile Watermarking Scheme for Authentication of JPEG Images



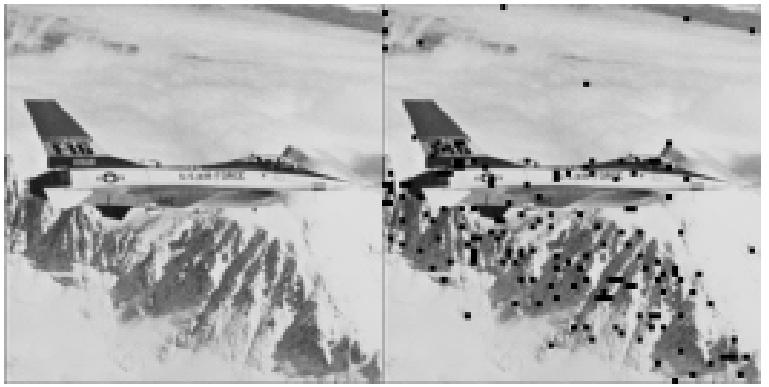
(a)



(b)



(c)



(d)

Attacked image and corresponding authentication result image (Airplane image) (a) blur attack, (b) sharp attack, (c) contrast attack, and (d) Gaussian lowpass filter attack.

❖ *Experiment 2:*

- *Detection of Malicious Manipulation:*
  - add additional dog
  - number plate was modified from “8J-9032” to “8O-9039”
  - remove “ baby in car ” logo

Manipulated and authentication result images (Car image) (a) The manipulated image, (b) The authentication result image.

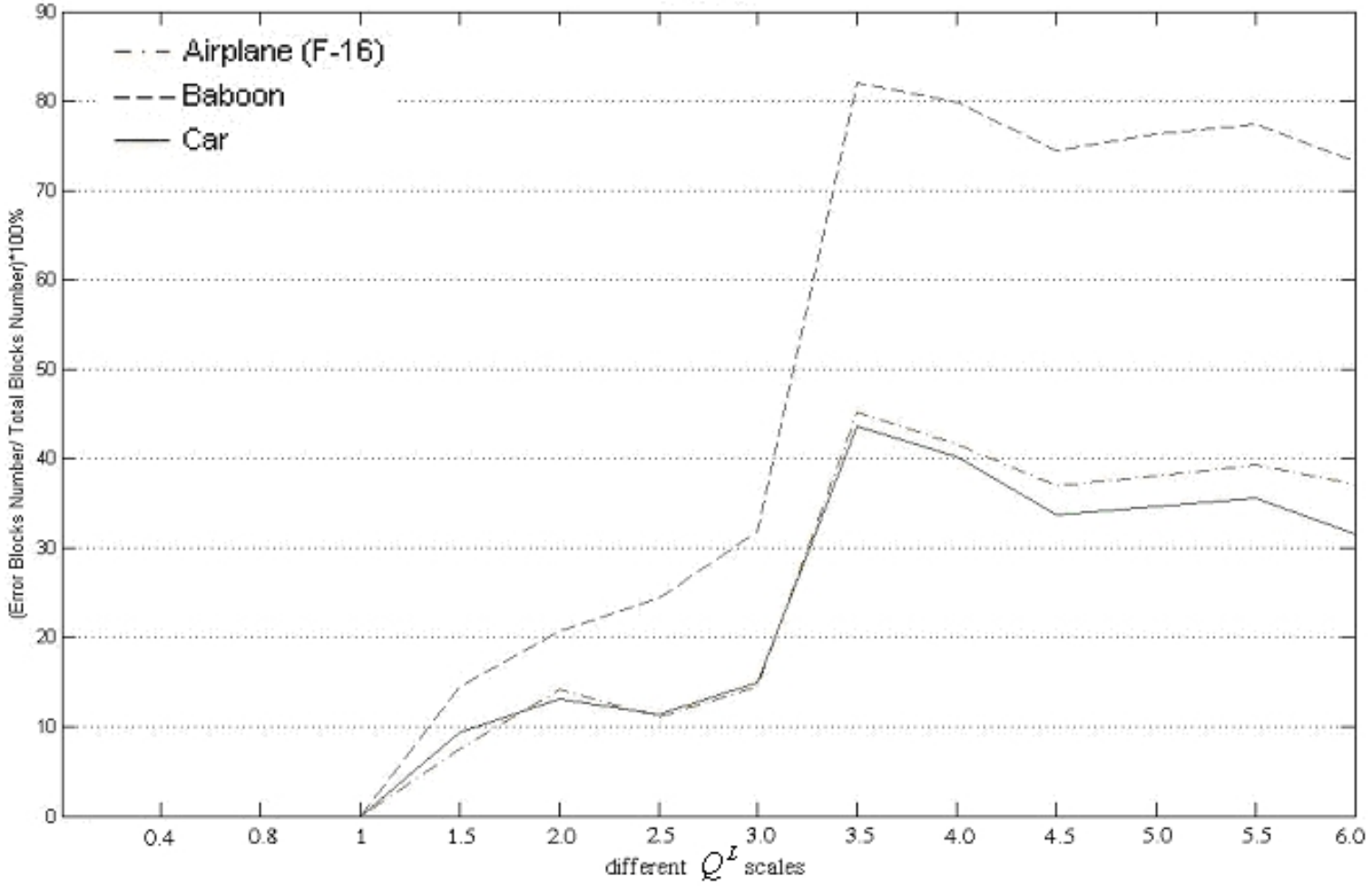
❖ *Experiment 3:*

- *Detection of JPEG Lossy Compression:*
  - The JPEG quantization matrix Q^L that corresponding to a given LAJQ was set to the well-known quantization table as follows

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

quantization table

4. Semi-Fragile Watermarking Scheme for Authentication of JPEG Images



Relationship between the error block ratio (error block ratio = error block number / total block number) and different Q^L scales.

Outline

5 **Image Authentication Scheme for Resisting the JPEG, JPEG2000 Compression and Scaling**

6 **Conclusions and Future Works**

5. Image Authentication Scheme for Resisting the JPEG, JPEG2000 Compression and Scaling

- Content-based digital signature method for verifying the image authentication under JPEG, JPEG2000 compression and scaling
- The invariant features, which are generated from the relationship among image blocks in the spatial domain
- Non-malicious manipulation is clearly defined to meet closely the requirements of storing images or sending them over the Internet

❖ *Definition of non-malicious manipulation*:

- (1) non-malicious manipulation must preserve the meaning of the image content
  - is well defined, but interpreted differently in different semi-fragile image authentication schemes
- (2) the non-malicious manipulation must reduce the size of the original image file
  - JPEG compression
  - JPEG2000 compression
  - Scaling

5. Image Authentication Scheme for Resisting the JPEG, JPEG2000 Compression and Scaling

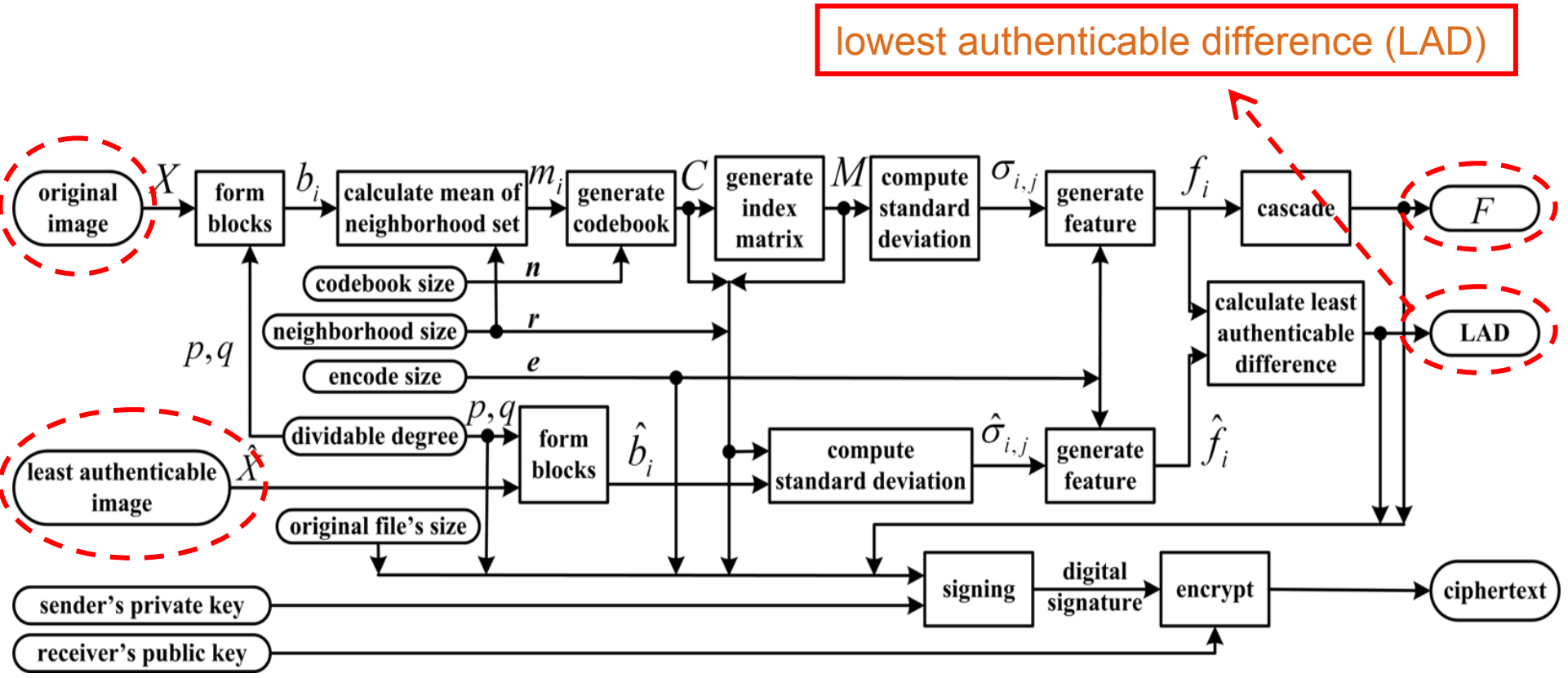


Diagram of image feature and cryptographic ciphertext generation methods

5. Image Authentication Scheme for Resisting the JPEG, JPEG2000 Compression and Scaling

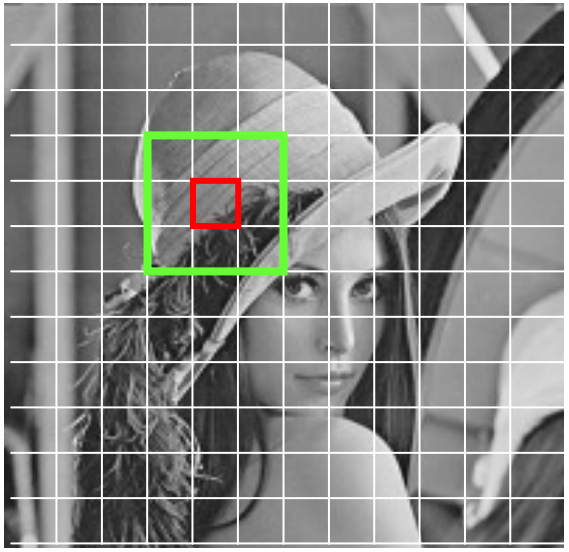
$f'_{53} = 29$: block feature of □ of LAI

↓ compute block feature difference

BFD (f_{53}, f'_{53})
$= |f_{53} - f'_{53}| = |18 - 29| = 11$

↓ compute least authenticable difference (LAD)

LAD = max (BFD (f_i, f'_i) for all blocks)



original image

$M[53] = 2$, $c_2 = 92$

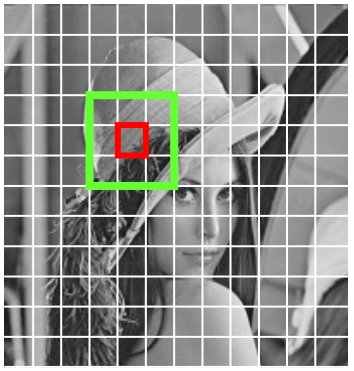
↓ compute the standard deviation of each blocks in □ 53

$\sigma_{53,0}$, $\sigma_{53,1}$, $\sigma_{53,2}$, $\sigma_{53,3}$, $\sigma_{53,4}$, $\sigma_{53,5}$, $\sigma_{53,6}$, $\sigma_{53,7}$, $\sigma_{53,8}$

max min

↓ compute the block feature of □ of original image

$f_{53} = [(\sigma_{53,4} - \sigma_{53,7}) / (\sigma_{53,2} - \sigma_{53,7})] \times 2^5 = 18$



least authenticable image (LAI)

5. Image Authentication Scheme for Resisting the JPEG, JPEG2000 Compression and Scaling

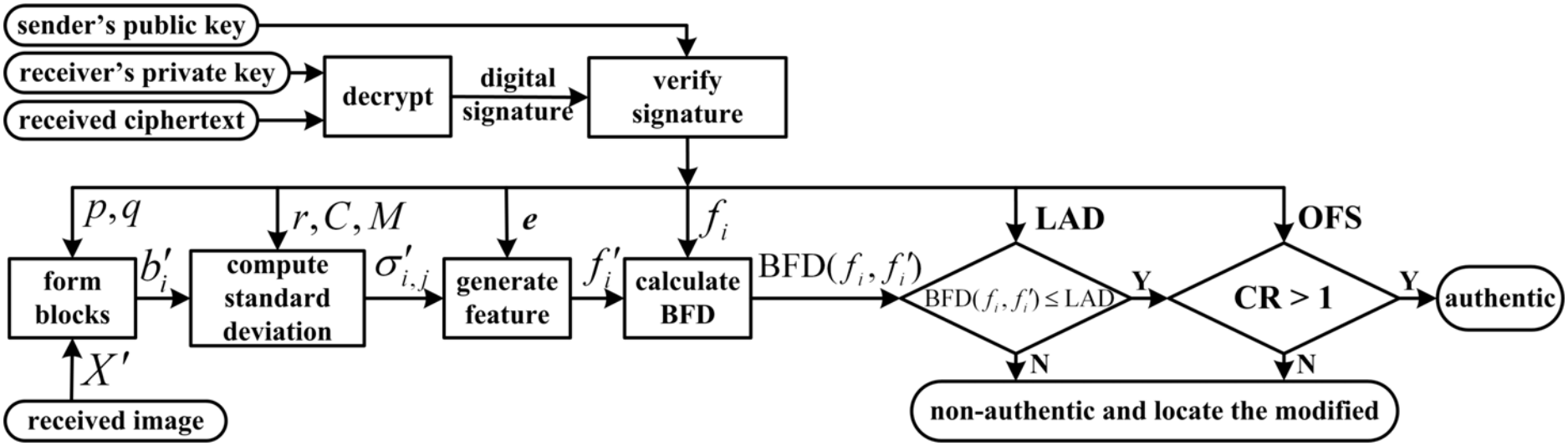


Diagram of image authentication method

Analysis and discussion

- 1. robustness of the proposed image authentication method
- 2. security
- 3. distinguishing non-malicious manipulations from malicious attacks

Experimental results

- Lena, Pepper and Fruits, with size 512×512 pixels, 24bits/pixel
- Image is divided into 32×32 blocks
- The well-known LBG VQ was adopted to generate the codebook
- The codebook size was set to 8, and the codeword length was 8 bits
- 25-neighborhood set was adopted, and the number of bits in the encoding feature was set to 5
- JPEG2000 compressed image that the Peak Signal to Noise Ratio (PSNR) closes to 34.0dB was adopted as the LAI

❖ Experiment 1: JPEG2000 compression

	Lena			Pepper			Fruits		
Bpp	PSNR	MBFD	CR	PSNR	MBFD	CR	PSNR	MBFD	CR
0.125	29.4	6.9	193.8	28.5	8.2	186.2	28.9	7.6	187.4
0.200	31.5	5.3	118.2	30.3	6.8	117.7	30.8	4.7	117.7
0.250	32.5	4.6	94.7	31.2	4.5	94.5	31.7	4.5	94.7
0.300	33.4	3.8	79.2	31.9	3.1	79.0	32.2	4.0	80.7
0.375	***34.2***	***2.9***	***63.3***	32.8	2.9	63.3	33.4	3.5	63.5
0.400	***34.6***	***2.2***	***59.7***	33.0	2.7	59.5	33.6	3.5	59.5
0.500	***35.4***	***2.2***	***48.1***	***33.7***	***2.5***	***47.7***	***34.7***	***2.9***	***47.7***
0.600	***36.4***	***2.1***	***39.7***	***34.3***	***2.1***	***40.1***	***35.5***	***2.4***	***39.9***
0.625	***36.6***	***2.1***	***38.2***	***34.5***	***2.0***	***38.4***	***35.6***	***2.4***	***38.2***
0.700	***36.8***	***2.0***	***34.1***	***34.9***	***2.0***	***34.1***	***36.2***	***2.0***	***34.3***
0.750	***37.1***	***2.0***	***32.0***	***35.2***	***2.0***	***31.9***	***36.6***	***2.0***	***31.8***
0.800	***37.3***	***1.7***	***30.0***	***35.4***	***1.9***	***29.9***	***36.9***	***1.9***	***30.0***
0.900	***37.8***	***1.7***	***26.7***	***35.7***	***1.9***	***26.6***	***37.5***	***1.7***	***26.6***

	Lena	Pepper	Fruits
LAD	**2.9**	**2.5**	**2.9**

- Bpp: bits per pixel
- maximum block feature difference (MBFD) = $\max(\mathrm{BFD}(f_i, f'_i) | 0 \le i < 2^p \times 2^q)$
- compression ratio (CR) = the file size of original image / the file size of manipulated image [Gonzalez 2002]

❖ *Experiment 2: JPEG compression*

	Lena	Pepper	Fruits
LAD	**2.9**	**2.5**	**2.9**

	Lena			Pepper			Fruits		
QF	PSNR	MBFD	CR	PSNR	MBFD	CR	PSNR	MBFD	CR
20	32.9	4.3	55.3	31.8	3.6	51.5	31.4	5.4	54.9
30	34.3	3.2	44.6	***33.6***	***2.5***	***41.8***	33.7	3.3	46.4
40	***35.1***	***2.2***	***37.5***	***34.2***	***1.5***	***35.0***	34.6	3.0	38.0
50	***35.8***	***1.6***	***32.3***	***34.8***	***1.5***	***30.5***	***35.3***	***2.8***	***32.3***
60	***36.5***	***1.4***	***28.1***	***35.3***	***1.2***	***25.8***	***36.0***	***1.6***	***27.8***
70	***37.3***	***1.2***	***23.2***	***35.9***	***1.0***	***21.2***	***37.0***	***1.2***	***22.9***
80	***38.5***	***1.2***	***17.8***	***36.8***	***0.8***	***16.3***	***38.5***	***1.1***	***17.9***
90	***40.8***	***0.5***	***11.4***	***38.8***	***0.7***	***10.2***	***41.2***	***0.6***	***11.8***

❖ *Experiment 3: Scaling*

- *SF = width of scaling image/ width of original image*
  = height of scaling image/ height of original image

	Lena	Pepper	Fruits
LAD	**2.9**	**2.5**	**2.9**

	Lena		Pepper		Fruits	
Scale factor (Image size)	MBFD	CR	MBFD	CR	MBFD	CR
31.3% (160×160 pixels)	6.4	10.2	8.1	10.2	10.8	10.2
37.5% (192×192 pixels)	5.8	7.1	6.7	7.1	9.8	7.1
50.0% (256×256 pixels)	***2.8***	***4.0***	4.5	4.0	9.6	4.0
62.5% (320×320 pixels)	***2.4***	***2.6***	2.9	2.6	4.0	2.6
68.8% (352×352 pixels)	***2.3***	***2.1***	***2.3***	***2.1***	3.8	2.1
75.0% (384×384 pixels)	***2.3***	***1.8***	***2.1***	***1.8***	***2.9***	***1.8***
87.5% (448×448 pixels)	***2.2***	***1.3***	***1.6***	***1.3***	***2.5***	***1.3***
93.8%(480×480 pixels)	***1.6***	***1.1***	***1.6***	***1.1***	***2.1***	***1.1***

❖ *Experiment 4: Additional image manipulations*

- (1) manipulated by PhotoImpact software package
- (2) manipulated by Matlab coding and the related coefficients were adopted from [Gonzalez 2002]
  - **smoothing spatial filtering** and **sharpening spatial filtering**

$\frac{1}{9}\times$

1	1	1
1	1	1
1	1	1

(a)

$\frac{1}{16}\times$

1	2	1
2	4	2
1	2	1

(b)

0	-1	0
-1	5	-1
0	-1	0

(c)

-1	-1	-1
-1	9	-1
-1	-1	-1

(d)

  - **lowpass frequency filtering** (Butterworth lowpass filtering (BLPF) of order 2, with cutoff frequencies (CF) at radii of 15, 30, 80 and 230, respectively)
  - **highpass frequency filtering** (Butterworth highpass filtering (BHPF) of order 2 with cutoff distance (CD) set 15, 30 and 80, respectively)

5. Image Authentication Scheme for Resisting the JPEG, JPEG2000 Compression and Scaling

(1) manipulated by PhotoImpact software package

	Lena	Pepper	Fruits
LAD	**2.9**	**2.5**	**2.9**

	Lena		Pepper		Fruits	
Manipulations	MBFD	CR	MBFD	CR	MBFD	CR
sharpening	14.7	1.0	9.9	1.0	16.4	1.0
blurring	23.1	1.0	13.6	1.0	22.8	1.0
Gauss blurring (radius=0.2)	0.2	1.0	0.8	1.0	1.2	1.0
Gauss blurring (radius=3.0)	23.5	1.0	14.6	1.0	24.0	1.0
adding noise (variance=1)	0.3	1.0	1.2	1.0	1.8	1.0
adding noise (variance=25)	9.1	1.0	6.9	1.0	15.3	1.0
brightness up 10%	27.5	1.0	24.2	1.0	26.4	1.0
brightness down 10%	27.9	1.0	24.8	1.0	31.0	1.0
contrast up 10%	9.2	1.0	8.1	1.0	17.9	1.0
contrast down 10%	9.3	1.0	8.7	1.0	31.0	1.0

5. Image Authentication Scheme for Resisting the JPEG, JPEG2000 Compression and Scaling

(2) manipulated by Matlab coding

	Lena		Pepper		Fruits	
Manipulations	MBFD	CR	MBFD	CR	MBFD	CR
smoothing spatial filtering (with mask1)	9.7	1.0	4.2	1.0	9.5	1.0
smoothing spatial filtering (with mask2)	6.8	1.0	3.7	1.0	7.5	1.0
sharpening spatial filtering (with mask3)	20.6	1.0	17.1	1.0	19.8	1.0
sharpening spatial filtering (with mask4)	25.4	1.0	23.6	1.0	29.3	1.0
lowpass frequency filtering (with CF=15)	25.4	1.0	22.5	1.0	27.2	1.0
lowpass frequency filtering (with CF=30)	23.1	1.0	14.4	1.0	23.8	1.0
lowpass frequency filtering (with CF=80)	6.8	1.0	9.2	1.0	11.8	1.0
lowpass frequency filtering (with CF=230)	1.8	1.0	2.1	1.0	1.0	1.0
highpass frequency filtering (with CD=15)	31.0	1.0	31.0	1.0	31.0	1.0
highpass frequency filtering (with CD=30)	31.0	1.0	31.0	1.0	31.0	1.0
highpass frequency filtering (with CD=80)	31.0	1.0	31.0	1.0	31.0	1.0

	Lena	Pepper	Fruits
LAD	**2.9**	**2.5**	**2.9**

5. Image Authentication Scheme for Resisting the JPEG, JPEG2000 Compression and Scaling

	Non-malicious manipulations	Domain transformation
[Sun, Q. 2005]	JPEG2000 compression	Frequency (DWT)
[Schneider 1996]	JPEG compression	Not Assignable
[Lin 2001]	JPEG compression	Frequency (DCT)
[Lu C.-S. 2003]	JPEG compression	Frequency (DWT)
[Venkatesan 2000]	JPEG compression	Frequency (DWT)
Proposed scheme	JPEG compression JPEG2000 compression Scaling	Spatial Domain

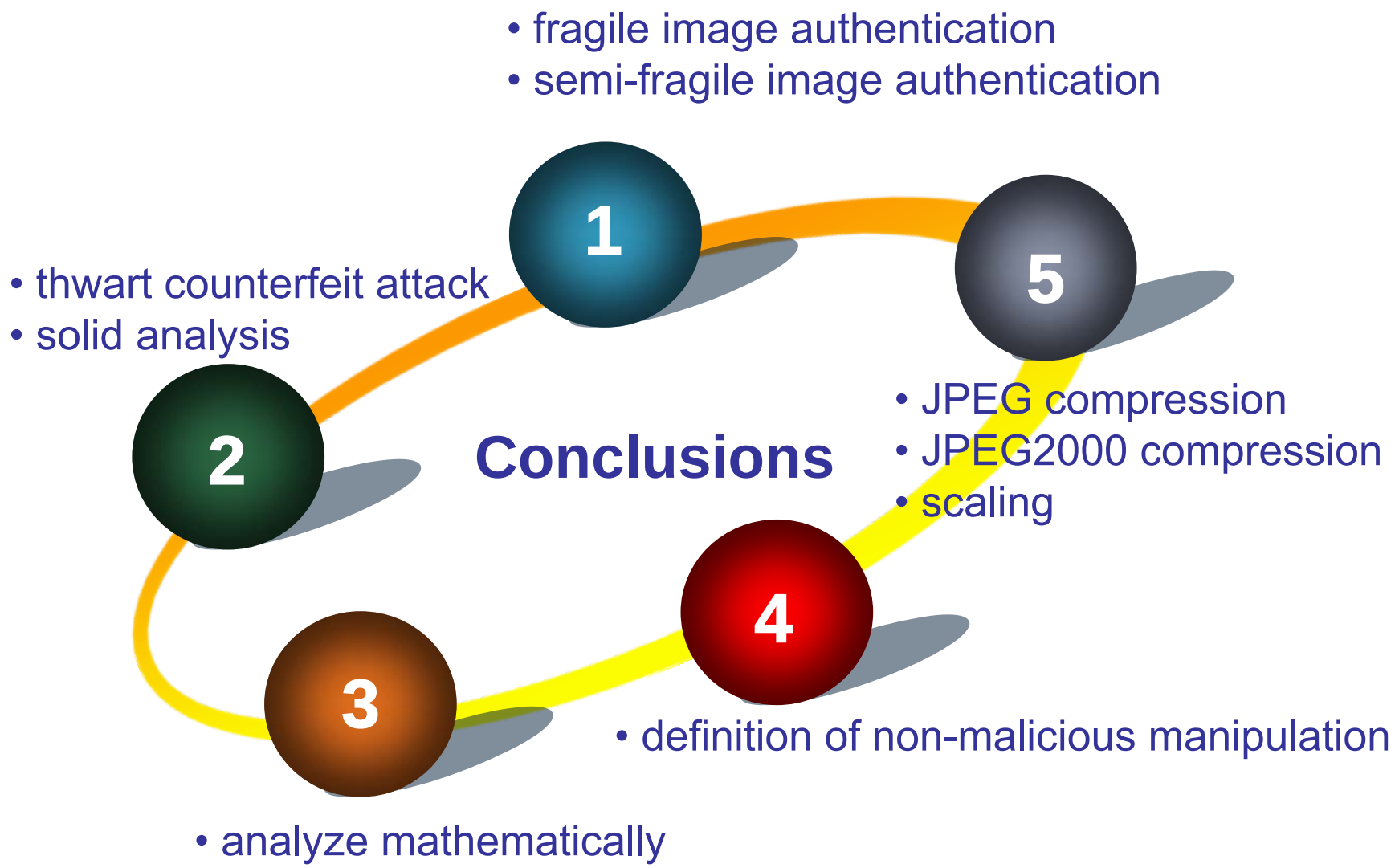
Comparison of the proposed scheme with related works about the application of non-malicious manipulations and the demanded domain transformation

Outline

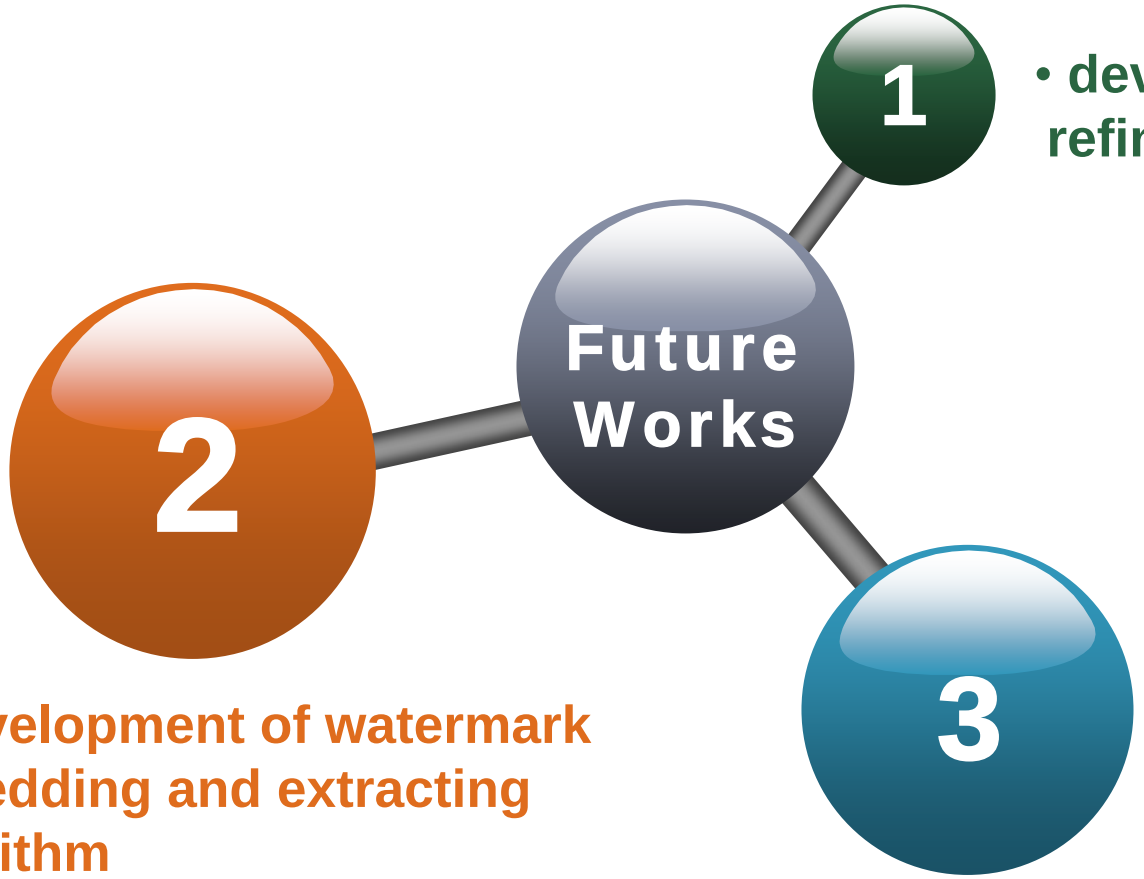
5 **Image Authentication Scheme for Resisting the JPEG, JPEG2000 Compression and Scaling**

6 **Conclusions and Future Works**

6. Conclusions and Future Works



6. Conclusions and future works



• development of refine algorithm

• development of watermark embedding and extracting algorithm

• development of tolerating more acceptable non-malicious manipulations

Thank You Very Much

- VPS pair

= $(21753,19289,20695)_{10}$

= $(101010011111001, 100101101011001, 111000011010111)_2$

<return>

RSA

- RSA為目前最著名的公開金鑰密碼系統，是由三位MIT的學者Rivest、Shamir與Adleman(Rivest, Shamir, & Adleman, 1978)於1978年提出。RSA密碼系統可作為加解密、數位簽章、金鑰交換等之用，其安全性是建立於因數分解(factorization)的困難度。

❖ (1) 金鑰產生

- (i) 任選二個大質數*p*與*q*，其中*p*與*q*爲強質數，並計算 $n = p \times q$
- (ii) 任選一數*e*滿足$\gcd(e,(p-1)(q-1))=1$，並計算$d=e^{-1} \bmod (p-1)(q-1)$
- (iii) 公鑰爲(*e*, *n*)，私鑰爲*d*。(*p*與*q*在系統設置完成後即可捨棄)

RSA

- **(2) 加密程序(*m* < *n*爲明文)**
  - 計算密文: $c = m^e \bmod n$
- **(3) 解密程序**
  - 計算明文: $m = c^d \bmod n$
- **(4) 簽署程序(欲簽署文件爲*m*)**
  - 計算簽章: $s = m^d \bmod n$
- **(5) 驗證程序**
  - 簽章驗證式： $m = s^e \bmod n$

註： RSA簽章法爲第一個提出具有訊息回復(message recovery)功能的數位簽章法。此外，RSA的加密與簽署動作正好相反。用接收方的公鑰來加密，用自己的私鑰來解密；用自己的私鑰來簽署；用簽署者的公鑰來驗證簽章。爲了增加安全度，訊息簽署前可以先經過一個單向雜湊函數*h*的轉換再進行簽署，亦即 $s = h(m)^d \bmod n$

RSA

- 例子：(明文爲688)
  - p=47, q=71 → n=47×71=3337
  - e=79 → $d=e^{-1} \bmod (p-1)(q-1)=79^{-1} \bmod 3220 = 1019$
  - 加密：$c=688^{79} \bmod 3337=1570$
  - 解密：$m=1570^{1019} \bmod 3337=688$

註： RSA的安全度建立於分解大合成數n 的困難度。A. Lenstra(1994)已可成功地分解出RSA 129位數。據學術界評估，目前應可有效地分解出RSA 135位數(約400位元)。因此，爲確保至少五年內之安全度需求，建議RSA的金鑰長度(亦即模數n 的大小)要達到1024位元以上才算達到安全。

6. Conclusions and Future Works

Future Works

- (1) Development of refine algorithm
  - if there are some blocks which have not been verified for authenticity and integrity, so the received image is suspect
  - two methods are available to solve the problem. One is re-transmission of the image and the other is to repair the modified portions

6. Conclusions and Future Works

Future Works

- (2) Development of watermark embedding/extracting algorithm
  - the sender must transmit an image and an extra authentication signature to the receiver
  - the difficulty for the development of the watermark embedding/extracting algorithm is that the extracted watermark must exactly equal to the embedded watermark after non-malicious image processing

6. Conclusions and Future Works

Future Works

- (3) Development of tolerating more acceptable manipulations
  - should more closely examine robust solutions under the proposed framework to tolerate more acceptable non-malicious manipulations combining JPEG, JPEG2000 compression, scaling, and others, e.g. scaled JPEG-compressed images, or scaled lowpass-filtering image
  - Complete derivation

Publication List

A. Refereed Papers

- 1. Chih-Hung Lin and Wen-Shyong Hsieh, ”Applying Projection and B-spline to Image Authentication and Remedy,” *IEEE Transactions on Consumer Electronics*, Vol. 49, No. 4, pp. 1234-1239, Nov. 2003 (SCI)
- 2. Chih-Hung Lin and Wen-Shyong Hsieh, ”Applying Statistics Ogive to Semi-Fragile Authentication of JPEG Images for Communication System,” *Tamkang Journal of Science and Engineering, An International Journal*, Vol. 9, No. 2, pp. 81-88, June 2006 (EI)
- 3. Chih-Hung Lin and Wen-Shyong Hsieh, ”Image Authentication Scheme for Resisting JPEG, JPEG2000 Compression and Scaling,” *IEICE Transactions on Information and Systems*, Vol. E90-D, No. 1, pp. 126-136, Jan. 2007 (SCI)
- 4. Chih-Hung Lin, Tung-Shih Su and Wen-Shyong Hsieh, "Semi-Fragile Watermarking Scheme for Authentication of JPEG Images", *Tamkang Journal of Science and Engineering, An International Journal*, Vol. 10, No 1, pp. 57-66, March 2007 (EI)

Publication List

B. Conference papers

(a) International Conference

- 1. Chih-Hung Lin, Ten-Chuan Hsiao, Hsien-Tsai Wu, Chin-Shan Ho and Cheng-Chien Hsu, "A Novel Semi-Fragile Image Authentication Method for JPEG Compression", *IEEE ICSS2005 International Conference On Systems & Signals*, pp.519-523, Apr. 2005.
- 2. Chin-Hung Lin, Ten-Chuan Hsiao, Hsien-Tsai Wu, Chin-Shan Ho and Che-Chia Ho, “A Novel Semi-Fragile Scheme for Image Authentication and Recover”, *IEEE ICSS2005 International Conference On Systems & Signals*, pp.365-369, Apr. 2005.
- 3. Chin-Shan Ho, Hsien-Tsai Wu, Chih-Hung Lin, Ten-Chuan Hsiao, Shing-Hua Ho and Yi-Zhi Huang, “A DSP Application for Measurement of Pulse Wave Velocity by Photoplethysmography and Electrocardiogram”, *IEEE ICSS2005 International Conference on Systems & Signals*, pp. 1477-1480, Apr. 2005.

Publication List

- 4. Chin-Shan Ho, Hsien-Tsai Wu, Deng-Maw Lu, Chih-Hung Lin, Shing-Hua Ho and Kun-Hsien Chou, “Development of a Measurement System for Electrocardiograms and Its Application to Remote Home Care”, *Proceedings of 2005 CACS Automatic Control Conference*, Nov. 2005.
- 5. Hsien-Tsai Wu, Chin-Shan Ho, Wei-Chuan Tsai, Ming-Chun Wang, Chih-Hung Lin and Hsuan-Kuang Chen, “Design of Portable Instrument for Physiological Pulse”, *Proceedings of 2005 CACS Automatic Control Conference*, Nov. 2005.
- 6. Tung-Shih Su, Chih-Hung Lin, Wen-Shyong Hsieh, “A Novel QoS-Aware Routing for Ad Hoc Networks”, *The 2006 International Conference on Wireless Networks (ICWN'06: June 26-29,2006, Las Vegas, USA) ((accept 2006/04/04))*

- 7. Chih-Hung Lin, Chin-Shan Ho, Ten-Chuan Hsiao, Hsiao-Fen Chien, Che-Chia Ho and Sheng-Lung Chien, "Semi-Fragile Image Authentication Scheme that robust to Compression and Scaling," Ming Chuan University International Academic Conference, Taoyuan, 2007. (published March 23, 2007)
- 8. Chih-Hung Lin, Chin-Shan Ho, Ten-Chuan Hsiao, Sheng-Lung Chien and Hsiao-Fen Chien, "The Shortest Movement Path System of Vehicles based on Image," Ming Chuan University International Academic Conference, Taoyuan, 2007. (published March 23, 2007)
- 9. Chin-Shan Ho, Hsien-TsaiWu, Chih-Hung Lin, Ten-Chuan Hsiao, Chia-Nian Shyi and Jiun-Liang Cheng, “Calculation of Continuous Heart rate during JOG and Recovery”, 2006 International Symposium on Biomedical Engineering (ISOBME), Taiwan.
- 10. Chin-Shan Ho, Hsien-TsaiWu, Jian-Jung Chen, Chu-Chang Tyan, Ten-Chuan Hsiao, Chih-Hung Lin and Chi-Kang Ho, “Design of Pulse Wave DataBase”, 2006 International Symposium on Biomedical Engineering (ISOBME), Taiwan.

(b) National Conference

- 1. Chih-Hung Lin and Wen-Shyong Hsieh, “Vector Projective Techniques for Integrity Verification in Fragile Watermarked Image”, 2003年資訊技術應用與發展研討會, pp.1-5, 2003.
- 2. Chih-Hung Lin and Sheng-Lung Chien , "A Semi-Fragile Image Authentication Method based on Wavelet Transform", 20th CVGIP, Aug 19~21 2007.
- 3. Chih-Hung Lin and Hsiao-Fen Chien , "A Semi-Fragile Image Authentication Method for Resisting JPEG and JPEG2000 Compression", 20th CVGIP, Aug 19~21 2007.