Benchmarking for SARI Image Authentication System

Lexing Xie, Kurato Maeno, Qibin Sun, Ching-Yung Lin, Shih-Fu Chang
ADVENT Group, Columbia Univ.

I. Introduction

In order to evaluate the performance of SARI image authentication system under common image storage, transmission and processing scenarios, the following test is basically performed from a consumer's perspective.

The issues of interest are: image quality after watermark embedding, robustness of authentication bits to JPEG compression, authentication sensitivity to malicious manipulation such as crop-and-replace, as well as widely-used but not directly oriented image processing methods such as low pass and median filtering, noise, brightness and contrast change, etc.

This test will also help to further improve SARI system or develop extended authentication schemes for multimedia.

II. Improvement from SARI 1.0 to 1.1

1 Better visual quality for synthetic and document image (see image quality section) By reversing the information bit to be embedded into all-white or all-black blocks.
2 Solved the non-convergence problem under border conditions.
3 Better system stability.

III. Image Quality Test

1 Objective test :
- Keep record of the image PSNR after watermarking embedding
- System parameter QR denotes the embedding strength related to maximum JPEG tolerate bound

2 Subjective test:
- Keep record of the maximum acceptable embed strength according to the judgments of the viewers
- Background of the image viewers and the monitors used are listed below:

Viewer No.1	image-processing	Trinitron 17'
Viewer No.2	image-processing	Sony Laptop
Viewer No.3	non-image-processing	Trinitron 17'
Viewer No.4	image-processing	Trinitron 17'

Figure 1. Test images (left->right, up->down):
Lena, Miss Tokyo, Café, LowMem Library,
Fruit, Clock, Reading, Strike, Insurance

Statistics in purple are from SARI 1.1, and statistics in black are from SARI 1.0.

Content Type			Human		Natural Scene & Building		Still Object		Synthetic		Document
Image Name			Lena	Miss Tokyo	Cafe	LowMem Library	Fruit	Clock	Reading	Strike	Insurance
Gray/Color			Color	Color	Color	Color	Color	Gray	Color	Color	Color
Size*			512*512	768*960	480*592	560*384	400*320	256*256	336*352	256*192	792*576
Objective Test PSNR (dB)	Auth only (3bits /block)	QR=0	48.7	48.3	48.9	48.9	48.7	50.1	51.4	48.7	51.6
		QR=1	46.4	45.7	46.6	46.7	46.4	46.7	48.4	45.4	48.6
		QR=2	44.6	44.0	44.9	45.0	44.6	44.6	46.2	43.3	46.6
		QR=3	43.0	42.3	40.2	43.5	43.1	42.9	44.7	41.7	45.0
		QR=4	39.8	39.1	33.2	40.3	39.8	39.2	41.4	38.3	41.7
	Auth + Reco (average: 13.1bits /block)	QR=0	42.6	43.6	37.9	39.6	41.7	41.7	36.2	40.2	40.6
		QR=1	41.9	42.5	37.7	39.3	41.1	41.1	36.1	39.6	40.3
		QR=2	38.0	38.9	33.3	35.0	37.1	36.8	31.4	35.5	35.8
		QR=3	37.6	38.4	33.2	34.8	36.9	36.5	31.3	35.2	35.6
		QR=4	36.4	36.7	32.8	34.2	35.8	35.3	31.0	34.0	35.0
Subjective Test (max acceptable QR)	Auth only	No.1	2	3	3	3	4	3	1	3	4
		No.2	3	3	4	3	4	3	4	4	4
		No.3	2	4	4	1	1	3	0	4	3
		No.4	3	3	4	2	4	2	3	3	4
	Auth + Reco	No.1	2	1	1	1	3	2	0	1	1
		No.2	2	2	3	1	1	2	0	0	0
		No.3	3	3	2	3	2	3	0	4	3
		No.4	1	2	3	1	3	1	0	1	3

Table 1. Quality Test Statistics

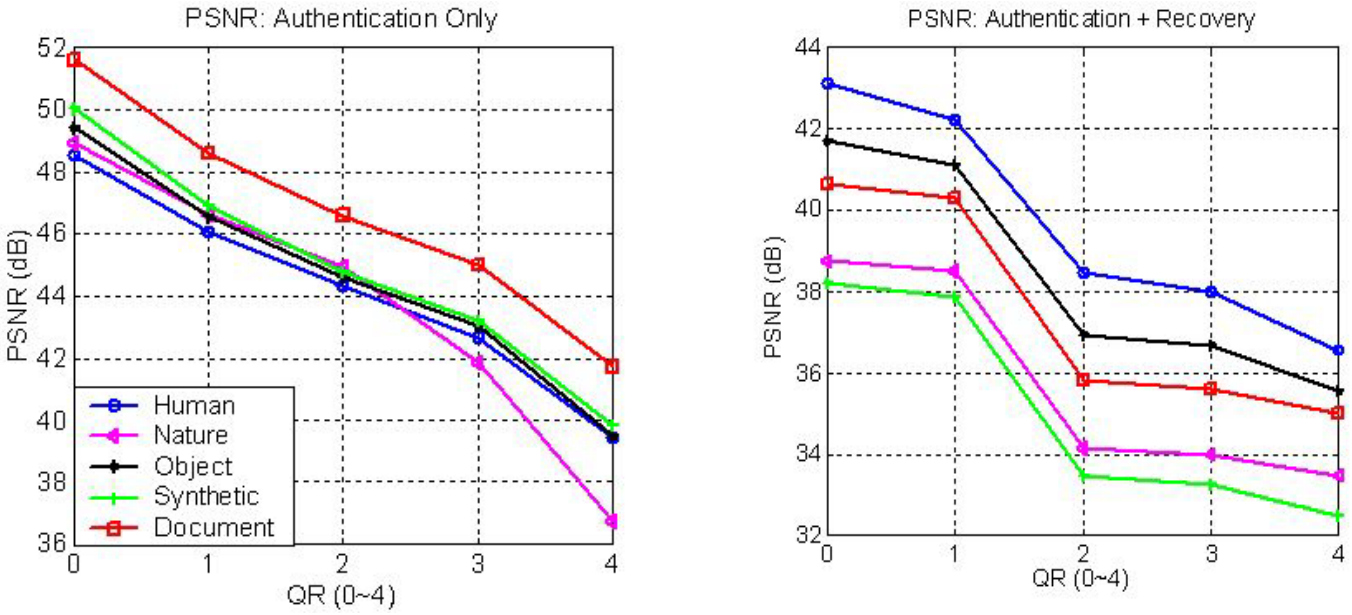

Figure 2. PSNR for different image types
(average value of the two images in this type)

Discussion on Image Quality

1 The changes are almost imperceptible for modest watermark strength QR= 0~2 (See Figure 3 below)

2 The embedding capacity of a natural image is generally larger than that of a synthetic image. This is because the former has more textural areas, thus the slight modification caused by authentication bits is less visible. The image quality of human, nature, and still object is generally better than that of synthetic and document image, and both the objective and subjective tests agree at this point.

3 The quality judgments vary among different viewers. This is because users pay attention to different features of an image and their tolerance bounds can be quite different. Moreover, different types of monitors have different display effects, e.g. the images that appear not acceptable on a Dell PC look just fine on a Sun Workstation.
In order to better suit the need of prospective user, extensive test is suggested among a specific user group before an general quality bound is decided.

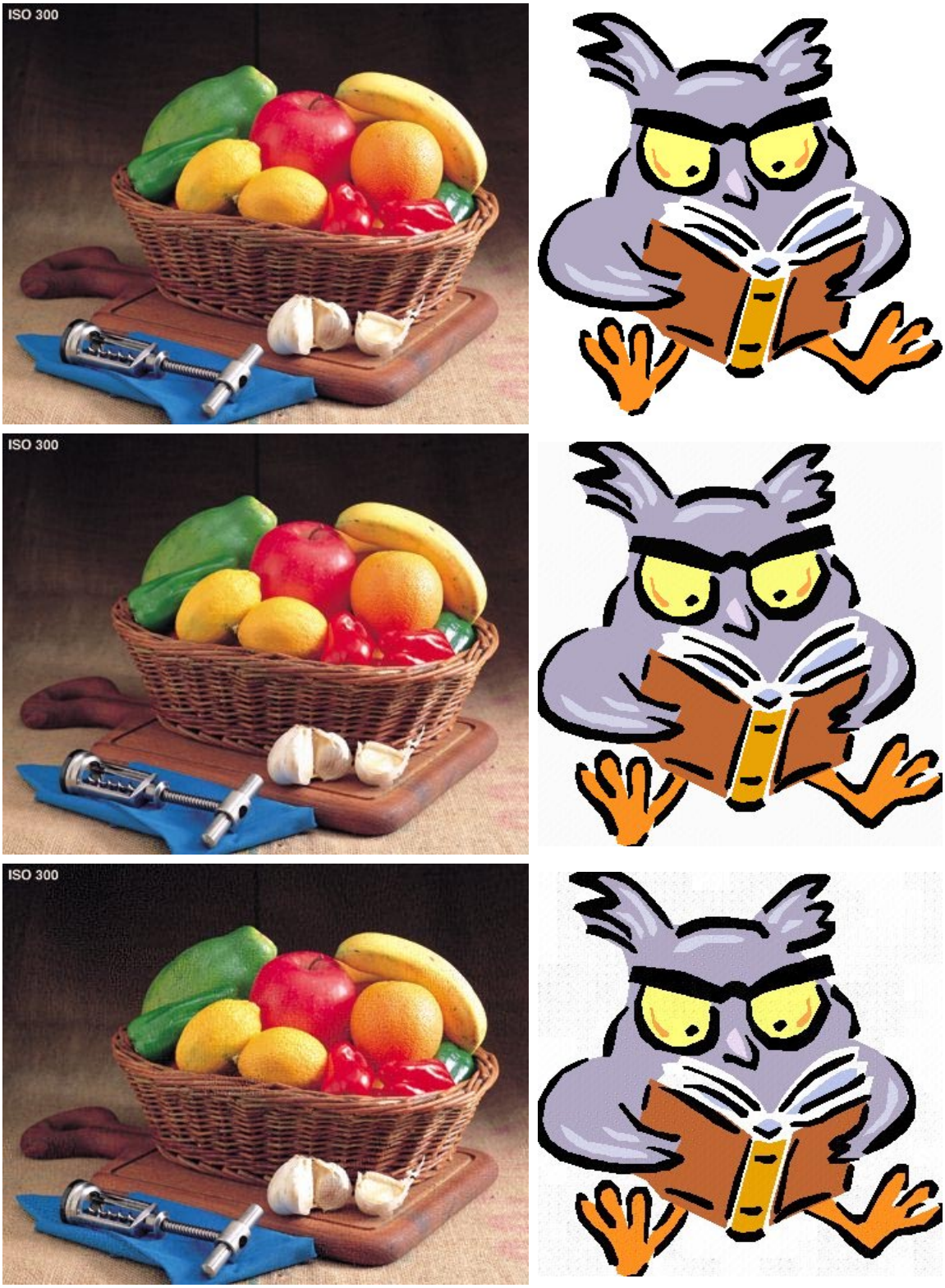

Figure 3. Embedding of different image types
Better case, Fruit: (top->down) original, auth only QR=1, auth+re, QR=3
Worse case, Reading: (right: top->down) original, auth only QR=1, auth+re, QR=0

IV. Performance Test

Experiment Condition

1 Maximum Embed Strength
Maximum QR value (embed parameter) of acceptable visual quality (chosen by 3 different viewers on 3 different monitor), and its corresponding PSNR
- A ---------- Authentication Only
- A+R ------ Authentication + Recovery

All experiment below are carried on to Authentication only watermarked images because authentication is the primary aim of the algorithm and recovery is complementary
The tool of all compressions and image processing is Photoshop5.0 to directly address user's application scenario.

2 JPEG
Minimum PhotoShop JPEG quality factor (1~10) the watermark can survive under maximum embed strength and QR=4 (authentication only), respectively

3 Manipulation
Whether the authenticator is sensitive to 1-pixle change or mass crop-&-replacement.
Case under QR=4 (maximum robustness)

4 Brightness, Contrast and Gaussian Noise
Adjustments to selected area, test both BMP and JPEG format
Case under QR=4 (maximum robustness)

4.1 JPEG Compression and Crop-replace

Content Type			Human		Natural Scene & Building		Still Object		Synthetic		Document
Image Name			Lena	Miss Tokiyo	Cafe	LowMem Library*	Fruit	Clock	Reading	Strike	Insurance
Gray/Color			Color	Color	Color	Color	Color	Gray	Color	Color	Color
Size*			512*512	768*960	480*592	560*384	400*320	256*256	336*352	256*192	792*576
Total # of Embedded Bits	A (3bits/block)		12,288	34,560	13,320	10,080	6,000	3,072	5,544	2,304	21,384
	A+R		47,240	109,514	88,751	52,868	24,616	11,686	34,033	10,474	90,968
max Embed Strength	A	QR	3	3	4	2	4	3	2	3	3
		PSNR	43.0	42.3	40.2	45.0	39.8	44.7	42.5	43.8	45.0
	A+R	QR	1	1	3	1	3	0	0	1	1
		PSNR	41.9	42.5	33.2	39.3	36.9	36.2	34.2	39.6	41.3
JPEG (A)	max(ED)		3	3	3	4	1	4	3	3	4
	QR=4		1	2	2	2	1	2	2	2	2
Manipulation	1-pixle		Y	Y	Y	Y	Y	Y	Y	Y	Y*
	crop		Y	Y	Y	Y	Y	Y	Y	Y	Y

Notations :
Y--- Authenticator alarm at the exact location N---- Authenticator no alarm
* Tested under better visual quality (QR=2)

* Size after watermark embedding (maybe slightly cropped to integer times of 16 or 8 during embedding process)
* Test under better visual quality

Table 2. Performance under JPEG Compression and Crop-Replace

Notes

1 JPEG Compression:

- All the information bits embedded in the image can be exactly reconstructed without any false alarm after JPEG compression.
- We observed similar results from other JPEG testing using XV, PhotoShop 3.0, PaintShop Pro, MS Paint, ACD See32, Kodak Imaging, etc.
- Statistics here conform with the robustness chart (QR 0~4) at http://www.ctr.columbia.edu/sari/performchart.html
- For instance, for image Lena, watermark with strength QR=4 survives Photoshop 5.0 Quality Factor 1 - 10.
- Watermarks embedded by using maximum invisible subjective embedding strength (max ED) can survive JPEG compression 3-10. This result is even better than predicted.

2 Crop-and-Replace:

Authenticator is quite sensitive to this kind of manipulation.
It can properly detect the change up to 1 pixel accuracy, and it is very effective in detecting the change of visual meaning, as shown in Figure 4.

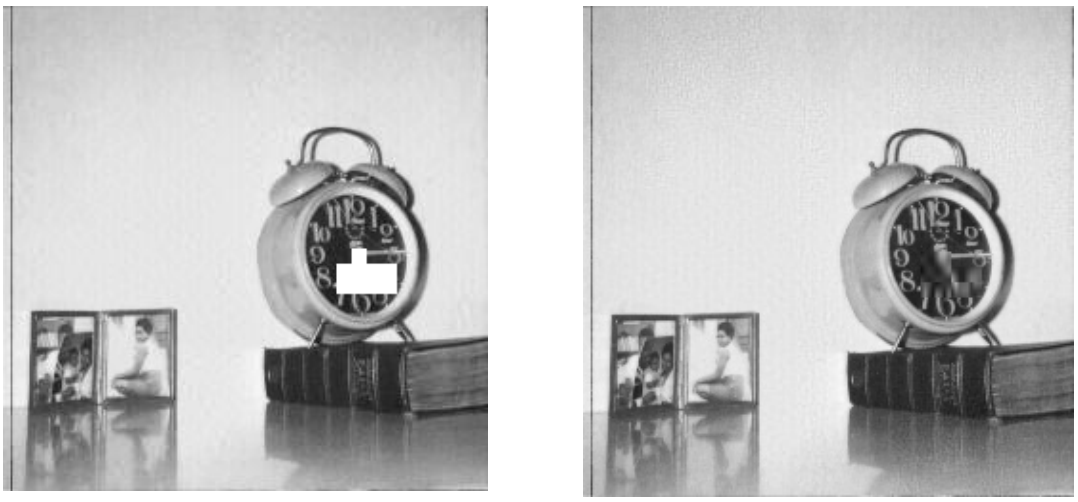

Figure 4. Detection and Recovery of Crop-and-Replace upper left: original; upper right: manipulated; lower left: authentication output; lower right: recovery output

4.2 Image Operations

Note: the image operations are not directly addressed in this authentication scheme, and these tests are carried on for reference purpose.

Content Type		Human		Natural Scene & Building		Still Object		Synthetic		Document
Image Name		Lena	Miss Tokiyo	Cafe	LowMem Library*	Fruit	Clock	Reading	Strike	Insurance
Gray/Color		Color	Color	Color	Color	Color	Gray	Color	Color	Color
Size*		512*512	768*960	480*592	560*384	400*320	256*256	336*352	256*192	792*576
Bright +1	BMP	Y*	Y	Y*	Y*	Y*	Y*	Y*	Y*	Y*
	JPEG	Y*	N	Y	Y*	Y*	N	Y*	N	N
Contrast +1	BMP	Y*	Y	Y*	Y*	Y*	Y	Y	Y*	Y
	JPEG	Y*	N	N	N	Y*	N	N	N	N
Gaussian Noise 1	BMP	Y*	Y*	Y*	Y*	Y*	Y*	Y*	Y*	Y*
	JPEG	Y*	N	N	N	N	N	Y*	Y	N
Smooth	Blur	Y	Y	Y	Y	Y*	Y*	Y	Y*	Y
	Median1	Y*	Y	Y	Y	Y	Y	Y	Y	Y

Notations :
Y-- Authenticator alarm at the exact location Y* -- Authenticator alarm but might not at the exact location N---- Authenticator no alarm
* Tested under max embed depth, i.e. QR=2
* Size after watermark embedding (maybe slightly cropped to integer times of 16 or 8 during embedding process)

Table 3. Performance under Image Operations

Notes

1. Common Image Operations
   - Blur or Median Filter: (minimum extent) the authenticator detects change
   - Gaussian Noise: (minimum extent) the authenticator detects change
     If further compressed to JPEG, usually no change detected because compression cancelled out the slight difference introduced by GN

- Brightness or Contrast Change: Authenticator detects change
  Sometimes JPEG compression will cancel the difference, and sometimes alarm blocks are misplaced

2. Small scale tests have also been done on skew, geometry transformation, etc.
   And the result shows authenticator will recognize these changes and issue global alarm.
3. The Recovery Issue:
   - Recovery can be regarded a bonus to the large embedding capacity, and the recovered part is a scaled down version with a quality similar to JPEG generic quality factor 25.
   - Recovery bits may be destroyed when the image is modified at several different places

The designer's comment (C.-Y. Lin): There might be no good trade-offs in setting a threshold to distinguish these operations from malicious operations. The difficulty is that, for instance, to survive these operations in a 512x512 image, the probability of false alarm (Pfa) in each coefficient should be smaller than 1/12288. This is not likely to happen in the presence of quantization, because even a small Gaussian noise added in the coefficients near the threshold boundary may introduce large distortion after quantization. Some mathematical analysis can be found in http://www.ctr.columbia.edu/sari/performchart.html reference papers [1] and [3].

For further technical details, please refer to: http://www.ctr.columbia.edu/sari
and Ching-Yung Lin, Shih-Fu Chang, "Semi-Fragile Watermarking for Authenticating JPEG Visual Content", SPIE 2000 (pdf)
For questions etc. contact: Lexing Xie <xlx@ctr.columbia.edu>