Joint SVD and QR Codes for Image Authentication

Wen-Chuan Wu[1*], Chi-Shiang Chan[2], Chih-Yang Lin[3,4], and Zi-Wei Lin[1]
[1]Dept. of Computer Science & Information Engineering, Aletheia University, Taipei, Taiwan
E-mail: au4387@au.edu.tw
[2]Dept. of Applied Informatics & Multimedia, Asia University, Taichung, Taiwan
E-mail: CSChan@asia.edu.tw
[3]Dept. of Bioinformatics and Medical Engineering, Asia University, Taichung, Taiwan
E-mail: andrewlin@asia.edu.tw
[4]Dept. of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan
[*]Corresponding Email: au4387@au.edu.tw

***Abstract*—Image authentication is an important technology to protect image content integrity. This paper proposes an image authentication method, which regards the stable singular values as significant authentication data and represents them in the form of QR codes. With the help of QR codes, the authentication data will be complete and correct even though the codes were slightly dirty or damaged. Experimental results showed that the proposed scheme is able to extract the correct authentication data out of QR codes under some attacks and to localize the tampered areas. Moreover, qualities of the authenticated image and the recovered image are superior to the previous method.**

I. INTRODUCTION

Image authentication is a kind of data protection techniques, used to confirm the integrity of digital images [8]. When image data are transmitted or stored using a network, we can use image authentication to detect whether an image has been modified or counterfeited. We call this process as tamper detection. Moreover, it is called data recovery to restore those modified regions in an image to its original state. Current image authentication techniques are classified into active and passive authentication schemes. Active authentication [1-4,7-9] involves protecting an image from being counterfeited before it is transmitted on the network. In this category, an authentication data is used to determine whether an image has been counterfeited. On the contrary, passive authentication [6] adopts images' inherent features to detect digital tampering locations, without requiring extra information.

Walton proposed an active authentication method [7], which applied checksum to perform modular operation on the most significant bits (MSBs) of each image pixel and regarded that results as image authentication information, embedding them into the LSB of pixels. But, this scheme is not secure, which allows attackers to maintain the checksum result without modifying the LSB. Wong et al. proposed a block-based image authentication scheme [9] later to solve Walton's shortcomings and make it safer. Chen and Wang [4] used fuzzy c-means clustering to generate the association among image blocks. This association was then used as an authentication data of the image itself. Chan et al. [1] employed hamming codes to adjust image pixel bits for tamper detection of authentication data. In 2013, Chuang et al. [3] utilized vector quantization compression technique to detect tampered locations of an image. And, they further used these compression data to restore the tampered regions.

Subsequently, Chen and Chen developed a novel scheme [2] using 2D quick response (QR) codes.

QR codes provide added protection for authentication data. That is to say, the extracted authentication data are still correct and complete even if an image was tampered with and the QR code was partially lost. However, Chen and Chen's scheme required the original image in order to accurately indicate the tampered locations on the image. In this paper, therefore, the proposed scheme utilized the error correction capability of QR codes to address the foregoing shortcomings. The rest of this paper is organized as follows: Section 2 is the introduction of singular value decomposition (SVD). Section 3 presents the proposed image authentication scheme based on QR codes. Section 4 presents several experimental results to show the improvement of the proposed scheme. The last section presents our conclusions.

II. SINGULAR VALUE DECOMPOSITION

SVD is an important matrix decomposition technology in linear algebra. It is mainly used to extract the eigenvector of a matrix. Thus, it is widely applied in many researches and applications, such as signal processing, image compression, noise removal, and data embedding. For a digital image, it can be regarded as a matrix containing non-negative scalar values. Let X be a $n \times n$ matrix, then SVD operation can decompose X into 3 matrices, U, S, and V, using (1) as shown below. Note that U and V are $n \times n$ orthogonal matrices and S is an $n \times n$ diagonal matrix containing values only on the diagonal line. These non-zero values are referred to as singular values, where $s_1 \geq s_2 \geq \ldots \geq s_n \geq 0$. In particular, the value of s_1 is much larger than other singular values; therefore, the singular values farthest from s_1 are usually negligible. When modified S and the original U and V matrices are reverse-transformed, the recovered matrix is similar to the original X image matrix. This is the reason that singular values are stable and are not prone to the influence of other values. Another characteristic of SVD is that a singular value corresponds to the brightness of an image, and the singular vectors U and V correspond to geometric texture characteristics.

$$X = U \cdot S \cdot V^T = \sum_{k=1}^{n} u_k \cdot s_k \cdot v_k^T = [u_1, u_2, ..., u_n] \times \begin{bmatrix} s_1 & 0 & \cdots & 0 \\ 0 & s_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & s_n \end{bmatrix} \times [v_1, v_2, ..., v_n]^T \quad (1)$$

III. THE PROPOSED SCHEME

This section introduces the proposed scheme which aimed at addressing the shortcomings of Chen and Chen's method [2]. It consists of three procedures: the authentication data embedding procedure, tamper detection procedure, and image content recovery procedure.

A. Authentication Data Generation and Embedding

SVD is able to analyze the maximum capacity of a matrix element. Therefore, it was used in this paper to extract an image's important authentication data [5]. Figure 1 shows our proposed data generation and embedding process. First, LSB elimination is executed, in which (2) is used to clear the final bit of each pixel x_{ij} of an $N \times N$ original image X into zero. Next, image is partitioned into non-overlapping 8×8 blocks (B^m where m=1, 2, …, $N^2/8^2$). Each block B^m is performed on SVD to decompose into three matrices U^m, S^m, and V^m. From the S^m matrix, each block selects two singular values $s_1{}^m$ and $s_2{}^m$ only as block's authentication data. Finally, all of the first and second singular values are grouped together to form two authentication data Au_1 and Au_2, where $Au_1=\{s_1{}^1, s_1{}^2, \ldots, s_1{}^{N\times N/8\times 8}\}$ and $Au_2=\{s_2{}^1, s_2{}^2, \ldots, s_2{}^{N\times N/8\times 8}\}$. Then, Au_1 and Au_2 are encoded into QR code format.

$$x'_{ij} = x_{ij} - (x_{ij} \bmod 2), \text{ where } i, j = 1, 2, \ldots, N. \quad (2)$$

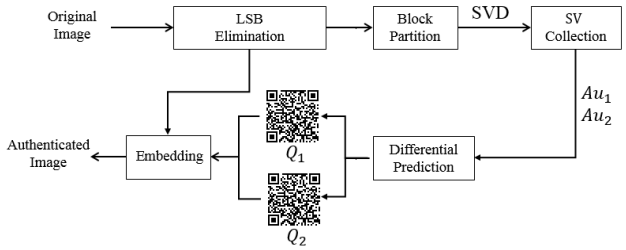
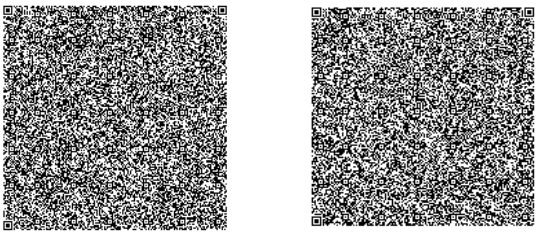


Figure 1. Flowchart of the proposed data generation and embedding procedure

The proposed scheme adopts differential prediction in order to reduce the volume of the QR codes. For the example of Au_1, the first singular value $s_1{}^1$ is a reference point to predict the next value; therefore, $s_1{}^2$ can generate a predicted error $e_1{}^1$ by using (3). This way is applied to predict the error values of the remaining singular values. Finally, there are $N^2/8^2-1$ error values are obtained and they are encoded into a 2D code Q_1 as shown in Figure 2. For Au_2, $s_2{}^1$ is also employed as a reference point. Next, our scheme embeds the two QR codes, Q_1 and Q_2, into the 1-LSB of each image pixel x'_{ij}. If the QR code pixel is white (denoting an intensity of 255), then the embedded image pixel x'_{ij} becomes $x^*_{ij}=x'_{ij}+1$; otherwise, if the QR code pixel is black (denoting an intensity of 0), then x'_{ij} becomes $x^*_{ij}=x'_{ij}$. This step is repeated until the two codes are both embedded in that image to finally obtain an authenticated image X^*.

$$e_1{}^m = s_1{}^{m+1} - s_1{}^m, \text{ where } m = 1, 2, \ldots, N^2/8^2-1. \quad (3)$$

$$e_2{}^m = s_2{}^{m+1} - s_2{}^m, \text{ where } m = 1, 2, \ldots, N^2/8^2-1. \quad (4)$$



(a)QR code of Q_1 (b) QR code of Q_2

Figure 2. An example of QR codes

B. Image Tamper Detection

Tamper detection is aimed at accurately detecting regions on an image that has been maliciously modified and altered. In this method, First is to extract 1-LSB from the pixels of an authenticated image and partitioned into two QR codes Q_1 and Q_2. Next, the embedded authentication data can be extracted by using QR decoder, but they were expressed as predicted errors; namely, $e_1{}^m$ and $e_2{}^m$. Therefore, (5) and (6) must be used to extract the original authentication data Au_1 and Au_2. Because QR codes have strong error correction capability, even if QR codes are somewhat incorrect, it can still be decoded to obtain complete authentication data, which are helpful in detecting the tampered locations.

$$s_1{}^{m+1} = s_1{}^m + e_1{}^m, \text{ where } m = 1, 2, \ldots, N^2/8^2-1. \quad (5)$$

$$s_2{}^{m+1} = s_2{}^m + e_2{}^m, \text{ where } m = 1, 2, \ldots, N^2/8^2-1. \quad (6)$$

In order to identify the tampered regions, LSB elimination and block partition shall be executed on an authenticated image in the beginning. Each non-overlapping 8×8 block B^{*m} is decomposed into singular values $s_1{}^{*m}$ and $s_2{}^{*m}$, which are then collected to form two authentication data Au^*_1 and Au^*_2. Next, the four sets of authentication data Au_1, Au_2, Au^*_1, and Au^*_2 are compared to determine possibly tampered regions on that image. Assuming that $s_1{}^m$ ($s_2{}^m$) in the Au_1 (Au_2) set does not equal $s_1{}^{*m}$ ($s_2{}^{*m}$) in the Au^*_1 (Au^*_2) set, then block B^{*m} is determined as a tampered region; otherwise, if $s_1{}^m$ ($s_2{}^m$) equals $s_1{}^{*m}$ ($s_2{}^{*m}$), then block B^{*m} has not been modified and is the correct location, as shown in (7). This step is repeated until all singular values are compared to yield a detected image. In the detected image, the tampered regions are marked in black and the correct regions are marked in white.

$$B^{*m} = \begin{cases} 1, & \text{if } s_1^m \neq s_1^{*m} \text{ or } s_2^m \neq s_2^{*m} \\ 0, & \text{if } s_1^m = s_1^{*m} \text{ and } s_2^m = s_2^{*m} \end{cases} \quad (7)$$

C. Image Content Recovery

After tamper detection procedure finishes, the next step is to recover image content of the tampered blocks to its original state. Each marked block is targeted to perform the following four steps of image content recovery using the said authentication data $Au_1=\{s_1{}^1, s_1{}^2, \ldots, s_1{}^{N\times N/8\times 8}\}$ and $Au_2=\{s_2{}^1, s_2{}^2, \ldots, s_2{}^{N\times N/8\times 8}\}$:

Step 1: Identify the correct location in a clockwise direction from the eight neighboring blocks within B^{*m}.

Step 2: Use the Euclidean distance to calculate the degree of similarity between the correct blocks and block B^{*m}. In (8), d_k denotes the difference in the singular values among the blocks, where a large d_k indicates a substantial difference between the two blocks.

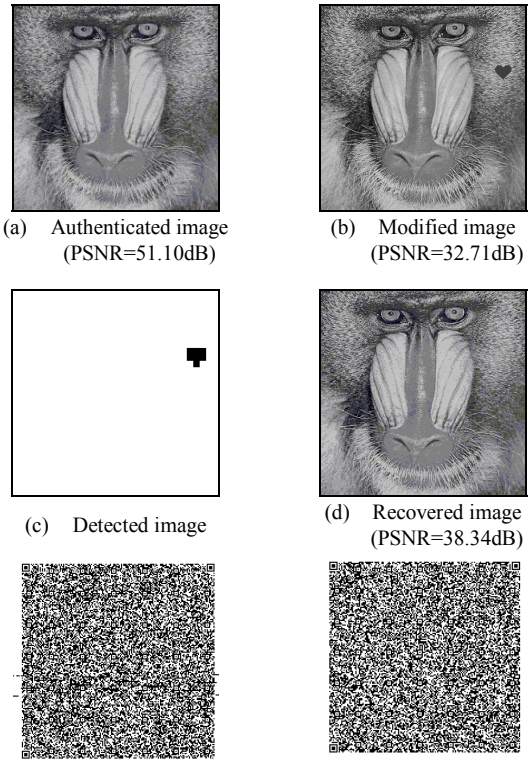
$$d_k=((s_1^m-s_1^k)+(s_2^m-s_2^k))^{0.5},\ k=1, 2, \ldots, 8. \quad (8)$$

Step 3: Select the smallest d_k from those resulting values and perform SVD on the block with the smallest d_k to obtain two matrices U and V. Then, compose the matrices U and V with singular values s_1^m and s_2^m to recover the content of block B^{*m}.

Step 4: Repeat Steps 1–3 again and again until all marked blocks are restored to get a recovered image.

IV. Experimental Results

Several experimental results are presented in this section to show the advantages of our scheme compared to Chen and Chen and scheme [2]. Here, six 256×256 grayscale images (Baboon, Pepper, House, Sailboat, Chart, and Jet) were used and each image was processed using our scheme to generate two singular values s_1 and s_2 as the authentication data. These data were expressed in the form of QR codes, whose sizes were both 175×175, and an error correction level of L was selected. In addition, an objective peak signal-to-noise ratio (PSNR) formula was adopted as the standard for assessing the qualities of the authenticated, modified, and recovered images.



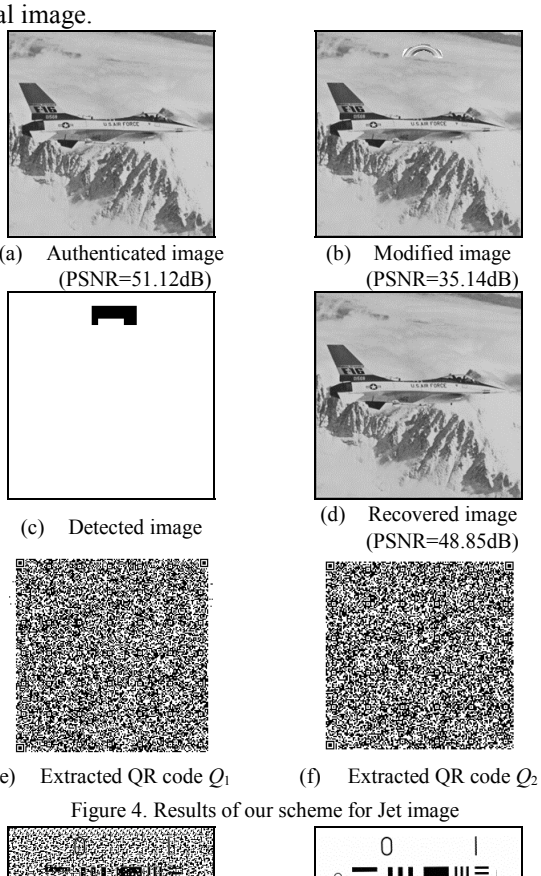
(a) Authenticated image (PSNR=51.10dB) (b) Modified image (PSNR=32.71dB)

(c) Detected image (d) Recovered image (PSNR=38.34dB)

(e) Extracted QR code Q_1 (f) Extracted QR code Q_2

Figure 3. Results of our scheme for Baboon image

Figures 3 and 4 are the resulting images for Baboon and Jet produced using our scheme. They show that the tampered areas can be correctly detected and that our scheme is able to almost restore the tampered regions back to original state. Tables 1 and 2 present the results of our scheme and Chen and Chen's scheme [2], respectively. It is clear that the quality of the authenticated images produced by our scheme is as high as 51dB, which is better than the previous scheme. Moreover, our scheme can detect the suspected regions and recover them whereas Chen and Chen's scheme failed to recover the image. In addition, Chen and Chen's scheme was ineffective in processing the image "Chart", which was nearly white and black, and this scheme produced an authenticated image with a quality of only 6.05dB. This result is attributed to the inapplicability of black and white images to be processed using DTC; therefore, an authenticated image produced using Chen and Chen's Scheme as shown in Figure 5(a) was observed. By contrast, the authenticated image in Figure 5(b) generated from our scheme looked almost the same as the original image.

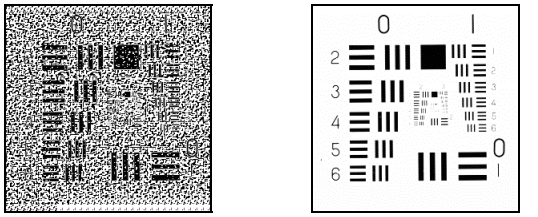


(a) Authenticated image (PSNR=51.12dB) (b) Modified image (PSNR=35.14dB)

(c) Detected image (d) Recovered image (PSNR=48.85dB)

(e) Extracted QR code Q_1 (f) Extracted QR code Q_2

Figure 4. Results of our scheme for Jet image



(a) Chen and Chen's scheme (b) The proposed scheme

Figure 5. Comparison of authenticated images using Chen and Chen's scheme[2] and the proposed scheme

Table 1. Results of our scheme for test images

Images	Authenticated image (dB)	Modified images (dB)	Recovered images (dB)
Baboon	51.10	32.71	38.34
Pepper	51.10	28.63	32.89
House	51.15	32.25	35.44
Sailboat	51.16	29.62	48.92
Chart	50.76	25.61	48.46
Jet	51.12	35.14	48.85

Table 2. Results of Chen and Chen's scheme for test images

Images	Authenticated image (dB)	Modified images (dB)	Recovered images (dB)
Baboon	43.91	30.12	N/A
Pepper	27.18	26.46	N/A
House	46.77	37.04	N/A
Sailboat	36.10	24.41	N/A
Chart	6.05	5.28	N/A
Jet	36.10	31.80	N/A

Note: N/A means that image is not available in the scheme [2]

V. CONCLUSIONS

SVD is effectively used to develop an image authentication system; it can protect the integrity of an image but it is likely to produce erroneous results. Therefore, an extra step of isolated block removal is required during SVD to remove erroneous data. In this paper, QR codes were used to replace the first and second singular values, which were embedded in the authentication data of an original image. Error correction capability of the QR code was leveraged to reduce the likelihood of error generation. The experimental simulation results revealed that the proposed scheme effectively and accurately pointed out the tampered locations on an image. Good-quality authenticated images were also generated. Furthermore, the proposed scheme is compared with previous image authentication scheme that also used QR codes. The proposed scheme can almost restore a tampered image back to its original state, without requiring the original image. In conclusion, the proposed scheme can protect the integrity of grayscale images effectively and efficiently.

ACKNOWLEDGMENT

This work was supported by the Ministry of Science and Technology, Taiwan, Republic of China, under the grant numbers MOST 104-2410-H-468-011.

REFERENCES

[1] C.S. Chan, "An Image Authentication Method by Applying Hamming Code," *Pattern Recognition Letters*, vol. 32, 2011, pp. 1679-1690.

[2] J.H. Chen and C.H. Chen, "Image Tamper Detection Scheme Using QR Code and DCT Transform Techniques," *International Journal of Computer, Consumer and Control*, vol. 1, 2012, pp. 61-68.

[3] J.C. Chuang, Y.C. Hu, C.C. Lo, and W.L. Chen, "Grayscale Image Tamper Detection and Recovery Based on Vector Quantization," *International Journal of Security and Its Applications*, vol. 7, 2013, pp. 209-228.

[4] W.C. Chen and M.S. Wang, "A Fuzzy C-Means Clustering-Based Fragile Watermarking Scheme for Image Authentication," *Expert Systems with Applications*, vol. 36, 2009, pp. 1300-1307.

[5] G. Felix and J. Nithya, "QR Code Hiding Using Histogram Shifting Method," *International Journal of Electronics Communication and Computer Engineering*, vol. 4, 2013, pp. 15-18.

[6] S. Mushtaq and A.H. Mir, "Digital Image Forgeries and Passive Image Authentication Techniques: A Survey," *International Journal of Advanced Science and Technology*, vol. 73, Dec. 2014, pp. 15-32.

[7] S. Walton, "Information Authentication for a Slippery New Age," *Dr. Dobbs Journal*, vol. 20, April 1995, pp. 18-26.

[8] W.C. Wu, "Subsampling-Based Image Tamper Detection and Recovery Using Quick Response Code," accept to *International Journal of Security and Its Applications*, Mar. 2015.

[9] P.W. Wong and N. Memon, "Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification," *IEEE Transactions on Image Processing*, vol. 10, 2001, pp. 1593-1601.