A Recoverable Image Authentication Scheme by Reed-Solomon Code

Wen-Chuan Wu

Dept. of Computer Science and Information Engineering, Aletheia University, Taiwan
au4387@au.edu.tw

Abstract

Generally, image authentication is able to verify artificial images and then to repair their damages. However, most image authentication schemes require hiding authentication data and recovery data both due to the abilities of tamper detection and data recovery. As a result, our work attempts to draw a portion of specific features as the important authentication and recovery data at the same time for the purpose providing a better image quality and confirming image integrity. We first encode an image by vector quantization technique to produce its compression codes. Then, an error correction code, Reed-Solomon code, is applied to protect the preceding compression codes against some malicious tampering attacks. Experimental results showed that the proposed scheme could yield a satisfactory image quality. Moreover, the usage of Reed-Solomon code is also able to resist tampering attacks and to correct recovery data.

Keywords: Image authentication, Tamper proofing, recovery, Reed-Solomon code, Vector quantization

1 Introduction

Because the rapid advancements of computer technology and the Internet, more and more data are converted into a digital format and these binary data are transmitted over public networks. Digitized data, images, audio, and videos especially, are easier to access, edit, and reproduce by a number of consumer electronic devices. Further, the data distributed over networks are more easily subjected to illegal modifies or attacks [11, 20], which is to tamper with data content arbitrarily. Hence, there is an urgent issue happened for data security and integrity. In general, cryptography is used to protect digital and sensitive data for the secure communication. However, the time-consuming and CPU-intensive encryption and decryption procedures are a little inapplicable to manipulate voluminous multimedia data [12].

Image authentication is one of techniques to protect the content of digital images. The beginning of this technology was to use digital signature [1, 2, 7] to draw features from images and then store as a file, which will be used later for authentication, carefully in a trusted third party [11]. Nowadays, most of image authentication schemes [3-5, 9, 12, 14-15, 17] are developed on fragile watermarking technique, which is characterized by the high fragility of watermarks. It is mainly to acquire the important image features as a watermark or authentication data, and then to embed these into the image itself in order to avoid false judgements. When it is necessary to verify whether a received image is not counterfeit, the embedded data will be drawn out and compared with features of the received image to identify the fake areas. Any slight tampering of image pixels will result in a damage of embedded data [15]. This process is so-called tamper detection. After it is judged as an illegal block, the fake area can be restored into its original state using recovery data, which is the so-called process of data recovery [4].

The earliest anti-forgery authentication method was proposed in [9], which applied checksum to perform modular operation on the most significant seven bits of each image pixel. The calculated results were then embedded in the least significant bit of each pixel, treating as the information of image authentication. In 2011, Chan [3] also proposed a pixel-wise image authentication method. That method utilized error-correcting hamming codes to rearrange image pixel bits for the purpose of a better repaired result. The schemes in [3, 9] are pixel-wise technique, in which the tampered pixels can be specified exactly in tamper detection procedure.

Another is block-wise authentication technique [4, 12, 14-15, 19]. An original image is separated into several small blocks, and then each block embeds with the watermark bits. Once tampering that image, the hided watermark bits will be destroyed and differ from the original data. The most typical block-wise authentication scheme for digital images was addressed by Wong and Memon [13], which put to use MD5 hash function to compress the block content and the hashed result is combined with the watermark to embed into image blocks. In addition to that, some works tried to

*Corresponding Author: Wen-Chuan Wu; E-mail: au4387@au.edu.tw
DOI: 10.3966/160792642018111906024

perform mathematical transformation, such as discrete cosine transform [6], discrete wavelet transform, and singular value decomposition (SVD) [12, 18], on blocks to get features. Wang and Tsai [14] performed in particular the fractal encoding technique on each block. Chen et al. [5] introduced block-based image secret sharing into the detection and recovery procedures. Moreover, schemes in [4, 8, 15] both utilize vector quantization compression, VQ for short.

VQ [16] has been considered as an efficient block-based lossy compression because of its simple decoding structure. Hence, this paper, which is partial of the scheme [11], develops an image authentication scheme upon VQ technique. It regards VQ encoding result as the authentication and recovery data of each block, and further employs Reed-Solomon code to defend the security of VQ results against tampering attacks. Reed-Solomon, RS for short, code [10] is a block-based error correction code to correct data errors and erasures occurred in digital communication and storage for a number of reasons. Its encoder adds extra redundant data, also named parity bits, for a block of digital data to detect and correct multiple symbol errors. When in the decoder, these redundant data are used to process each block and attempt to correct errors and recover the original data. Therefore, we will make good use of error correction capability of that code to secure VQ authentication data so as to improve the recovered image quality.

The rest of this paper is organized as follows: Section 2 introduces error-correcting Reed-Solomon code and a previous image authentication scheme [12]. The proposed image authentication scheme is presented in Section 3. Section 4 shows experimental results of our scheme, followed by a conclusion in Section 5.

2 The Related Works

In this section, we will introduce Reed-Solomon code [10] and review a previous SVD-based image authentication scheme [12] using quick response (QR) code, which proposed by Wu and Lin.

2.1 Reed-Solomon Code

RS code proposed by Reed and Solomon is a block-based error correction code, which have been applied to a large number of applications including wireless or mobile communications, digital television, and the popular two-dimensional quick response code [12]. Before storing in storage devices or transmitting over channels, it is highly suggested to perform error correction coding upon any data source in order to prevent noise and errors happened.

Figure 1 shows RS coding system, where the channel is influenced quite easily by impulse noise, lightning, electrical discharge, and so on. The RS encoder works to take a block out of digital data and adds extra redundant information. And, redundant information (or parity bits) is used to detect whether the received data was tampered with before; then, correct multiple errors that may have occurred in transmission and storage. Figure 2 presents a diagrammatical definition of RS(n, k) code. RS(n, k) means that the encoder takes original data of k symbols and adds parity symbols to form a message block of n symbols; on the side, the decoder is able to correct up to t symbols that contain errors.

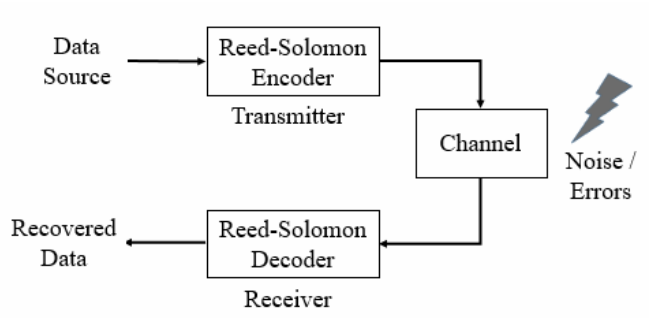


Figure 1. RS coding system

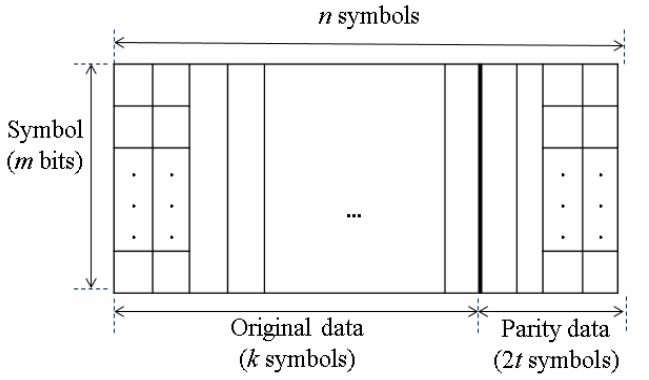


Figure 2. Definition of Reed-Solomon code

In the encoder of transmitter side, the code first divides the information sequence into many message blocks of k symbols, where each symbol is m bits, and then each block has $2t$ redundant parity symbols added to the end of k symbols to form a message block of n symbols. In general, it is specified as RS(n, k) with m-bit symbols, where $n = 2^m - 1$ and $k = n - 2 \times t$. Given a symbol size m=3, the maximum message length is $n = 2^3 - 1 = 7$. Assumed that the decoder can correct any t=1 symbols error in the message. Then, there are k=5 symbols being original data and 2 symbols being parity data in the message. Finally, the message block of 7 symbols is transmitted over a communication channel. Once some symbol was tampered with unauthorized modification, that RS(7, 5) decoder can still restore the message correctly due to that magnitude of modification is less than the value of t.

Noted that the higher the value of t is, the better the error correction capability but the more the redundant symbols will be; and vice versa. The number of

redundant symbols also affects the quality of the recovered image. In a word, RS code is provided with the capabilities of the largest possible code-minimum-distance and high error correction.

2.2 Wu and Lin's Scheme

In 2016, Wu and Lin proposed an SVD-based image authentication scheme [12], which utilizes the error correction of QR codes to restore authentication data. In fact, the QR code is provided with error correction feature by implementing a Reed-Solomon code to the original data. Figure 3 depicts the authentication process of Wu and Lin's scheme. In their scheme, there are two SVD-based schemes in total: Scheme-1 and Scheme-2. The difference between them is the number of involved singular values. Here, we only list the algorithm of Scheme-2 step by step in below:

Step 1: Clear 1-LSB of each pixel into zero.

Step 2: Partition the result into many 4 × 4 blocks and each block is performed on SVD operation. In each block, only the first singular value is collected to form a set of authentication data.

Step 3: Pair two neighboring values to calculate their mean values. Then, separate these into two sets.

Step 4: Apply differential prediction to the two sets for generating the corresponding predicted errors.

Step 5: Express two sets in QR code formats using a QR encoder.

Step 6: Embed the two QR codes into the 1-LSB of each image pixel. If QR code dot is white, then that pixel bit becomes "1"; otherwise, that pixel bit is still "0".

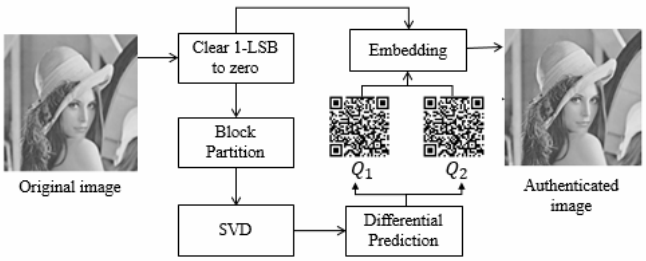


Figure 3. Flowchart of Wu and Lin's scheme [12]

In the end, an authenticated image also similar to the original one will be obtained. During tamper detection and data recovery process, the embedded QR codes are first extracted from each pixel of the authenticated image. Next, decode them to derive the involved authentication data. Compare these with the results produced from authentication data generation process on that authenticated image to detect where the possibly tampered blocks are. Once they are not the same, it means that some blocks are suspected as tampered regions. After that, it is targeted to adopt the first singular value, which keeps in QR codes, together with orthogonal matrices of the most similar neighbor in order to recover the content of each tampered block. Wu and Lin's scheme can accurately authenticate the integrity of digital images. However, the limitation of this scheme is the extent of tampering regions. Once the magnitude far exceeds the error correction limit of a QR code, it will be too difficult to read that QR codes such that this scheme fails to the tamper detection and data recovery process.

3 The Proposed Scheme

This section describes our image authentication scheme using Reed-Solomon code in order to protect authentication data and improve the recovered image quality. Our scheme consists of four procedures in sequence:

(1) authentication data generation;
(2) authenticated image generation;
(3) tamper detection;
(4) tampered image recovery.

Figure 4 shows the flowchart of our authentication scheme. In the proposed scheme, we apply RS(15, 9) code, which is able to correct 3 symbol errors at most, to protect VQ index values for image blocks.

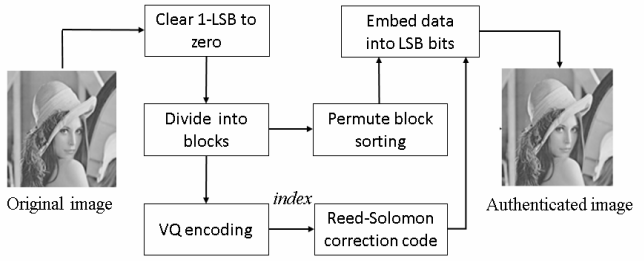


Figure 4. Flowchart of the proposed authentication

3.1 Authentication Data Generation

This procedure is to generate authentication data from an original image. Assume that the original image is the size of $M \times N$ pixels. First, clear the least significant 1 bit of each image pixel to zero. Then, divide resulting image into non-overlapping blocks B_i with 4 × 4 pixels, where i is the block ID. Each block is performed on the compression of VQ coding to get the corresponding index value, representing idx_i, in an index table. Figure 5 is an example of VQ encoding and decoding for a 2 × 2 block, where solid lines indicate the process of a VQ encoder and dotted lines indicate the process of a VQ decoder. When in the VQ encoding, a block is to search the closest codeword in a codebook by calculating Euclidean distance [4]. Then, the corresponding index of the found codeword is used instead of the original block. It is obvious in Figure 5 that the index of the most similar codeword is 115. Hence, the value is recorded in an index table.

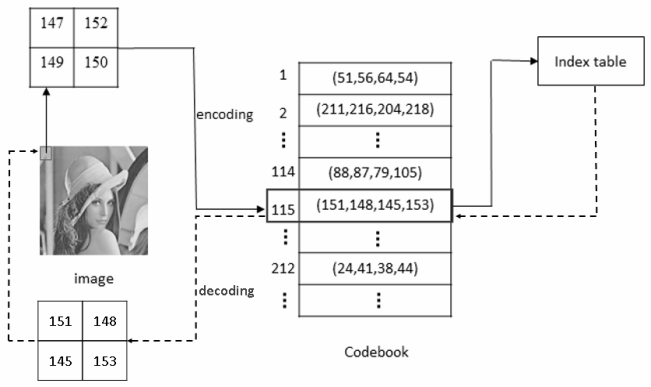


Figure 5. Flowchart of VQ encoding and decoding technique

In VQ decoding process, the codeword indexing 115 is taken from the codebook to reconstruct that 2 × 2 image block. It can be seen in Figure 5 that the rebuilt result is very similar to the original block. If there are 256 codewords in a VQ codebook, each image block B_i will generate an 8-bit index value idx_i, where that index is used to restore an extremely similar block. Hence, VQ index values can be treated as the important authentication and recovery data simultaneously for image blocks. In addition, we also disarrange the order of image blocks using a chaotic permutation for the purpose of data security.

3.2 Authenticated Image Generation

In order to protect the indices against modifying attack, our scheme then performs on Reed-Solomon code. Here, each 8-bit index idx_i is separated into two 4-bit values $I_{2\times i-1}$ and $I_{2\times i}$. The number of values in set I is twice as large as that of VQ indices, shown as follows:

$$I=\{I_1, I_2, \ldots, I_{2\times(M\times N)/(4\times 4)}\},$$
$$IDX=\{idx_1, idx_2, \ldots, idx_{(M\times N)/(4\times 4)}\}.$$

Supposed that the index value for the first block is 120 representing $(0111\ 1000)_2$ in binary form. In that case, values I_1 and I_2 are 7 in binary $(0111)_2$ and 8 in binary $(1000)_2$, respectively. Then, each round we pick eight 4-bit values and a 4-bit random as original data to produce their six 4-bit parity symbols by using a RS(15, 9) encoder. For a message block of fifteen symbols, we embed the earlier eight original data into the preceding eight pixels of four image blocks and embed six 4-bit parity symbols into the following eight pixels.

As shown in Figure 6, each four image blocks are used to carry the message of fourteen 4-bit symbols, where there are 32 bits being the original block index and 24 bits being the redundant parity bits. In other words, a total of 56 bits are hidden in four image blocks. Merely, there are eight LSBs, colored in gray dot, of image pixels not been carried data. Note that blocks B_i to be embedded are permutated beforehand as that referred to in the prior subsection. Take an example shown in Figure 7, where each value in it represents block number. For the block B_1, its 4-bit values I_1 and I_2 are embedded into the block B_3 while the two values in the block B_3 are embedded into the block B_8. After embedding, an authenticated image corresponding to the original image would be finally acquired.

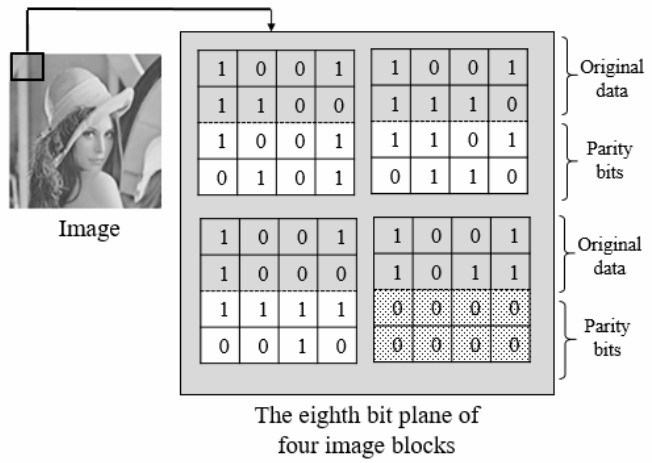


Figure 6. Concept of our data embedding

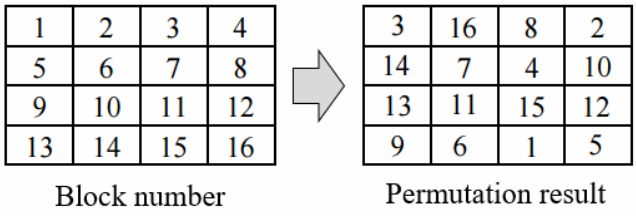


Figure 7. Example of block permutation

Figure 8 is an example to show the proposed authenticated image generation process more clearly. Supposed that there are four VQ indices, 134, 129, 36, and 249 for blocks B_1, B_2, B_3, and B_4. Then, we will get eight values from the four indices, that is to say 8, 6, 8, 1, 2, 4, 15, and 9 as shown in Figure 8. After a RS(15, 9) encoding, six values, 15, 13, 10, 0, 6, and 13, will be generated from the eight values along with a 4-bit random value 9. The eight values and the six parities are both the important authentication and recovery data, hence they should be recorded in the image itself. For the block B_1, 8 in binary $(1000)_2$ and 6 in binary $(0110)_2$ are embedded into the 1-LSB bits of the preceding eight pixels in the block B_3. And, the two parity values 15 and 13, representing in binary $(1111)_2$ and $(1101)_2$ respectively, are embedded into the 1-LSB bits of the following eight pixels in the same block B_3. It is not necessary to store the random value, so the last eight pixels in some block will not be modified.

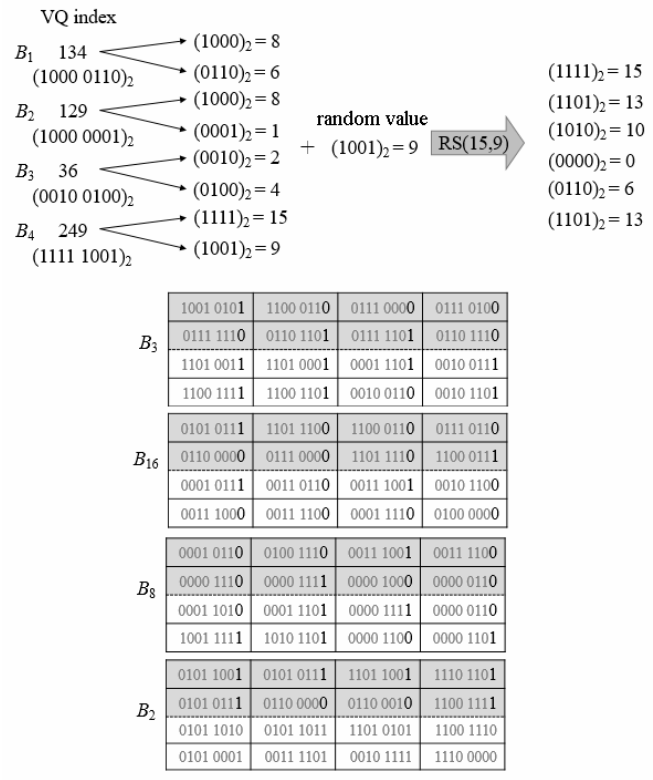


Figure 8. Example of authentication data generation for four blocks

3.3 Tamper Detection

The goal of tamper detection procedure is to verify whether a received image is a fake. Initially, the received image is permuted the same as the prior result in authenticated image generation. It is for each four blocks to extract 1-LSB bits from the preceding eight pixels of every block to form four 8-bit index values idx_i. For example, we can obtain idx_1, idx_2, idx_3, and idx_4 from blocks B_3, B_{16}, B_8, and B_2 in Figure 7. The following 8-LSB bits are also taken out from the three of blocks to be the recovery data. On the other hand, the received image is to clear the least significant 1 bit of each pixel to zero. Then the same operations, block partition and vector quantization coding, are executed to derive the index values idx'_i. In order to identify the possibly tampered blocks, it is necessary to compare the extracted indices idx_i with the value idx'_i. Once they are not the same as each other, then the i-th block is determined as a tampered one. In opposite, if the same, it indicates that the i-th block has not been tampered or modified before.

3.4 Tampered Image Recovery

A detected image is derived in the end of tamper detection, in which suspected tampered blocks are colored in black; or else, correct blocks are colored in white as the detected results shown in the following experiments. For those suspected tampered blocks, it is first to execute isolated block removal process to prevent possibly false tampering detection. The main reason is that the modified regions are usually larger and far away from one single block. For a tampered block, it was misjudged if an amount of neighboring blocks colored in black does not exceed the threshold tm. And, it is necessary to color that block in white. By sequentially processing each tampered block, a refined detection result will be acquired. The next step is to restore image content of tampered blocks by using RS(n, k) decoder. In Reed-Solomon decoder, the $2t$ parity symbols embedded in the following 8-LSB pixels of each block are used to correct the k symbols of index values. Under the error correction bound, the modified $\lfloor t/2 \rfloor$ index values can be corrected, and then further be used to recover image blocks by using vector quantization decoding. Hence, RS(15, 9) code in our scheme is able to correct one wrong block at most among each four blocks. Noted that in our scheme an authenticated image cannot undergo JPEG coding or be stored into other image formats because authentication data will disappear.

4 Experimental Results

Some experiments are showed to demonstrate performance of the proposed scheme. Five standard grayscale images with size of 256 × 256 pixels were test images in our experiments, which are “Barbara”, “Lena”, “Pepper”, “Sailboat”, and “Toys”. Each image was then processed using the proposed scheme and the previous SVD-based scheme [12] to generate the corresponding authenticated images. Here, we adopted PSNR as an objective metrics to evaluate visual qualities between an original image and other modified images. Generally speaking the higher PSNR value is, the better the quality of modified or recovered image will be, and vice versa.

First of all, we are interested in the results of isolated block removal process used in our tampered image recovery procedure. What a threshold value tm is appropriate? Figure 9 and Figure 10 present the results of recovered qualities and the amount of detected blocks, respectively, under distinct thresholds tm. It is very obvious from the two figures that values tm between 2 to 4 produced similar and good results. Considering the recovered quality and the actual detection results, hence, a threshold value of tm=3 is recommended for using in the following experiments. Figure 11 shows the tampered image and the detected results under distinct threshold values for test image “Pepper”. It is clear that there are many misjudged blocks appeared in the detected results using tm=0. Through the process of isolated block removal, our scheme is able to reduce the amount of misjudged blocks in detected results.

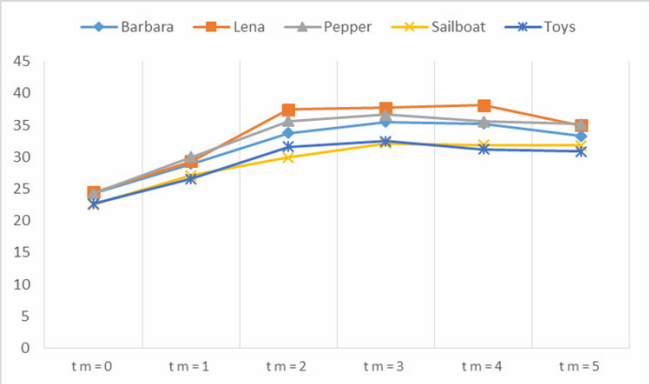


Figure 9. Recovered quality under distinct thresholds *tm*

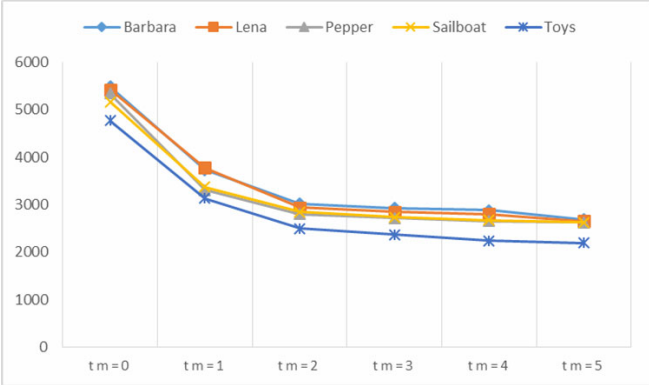
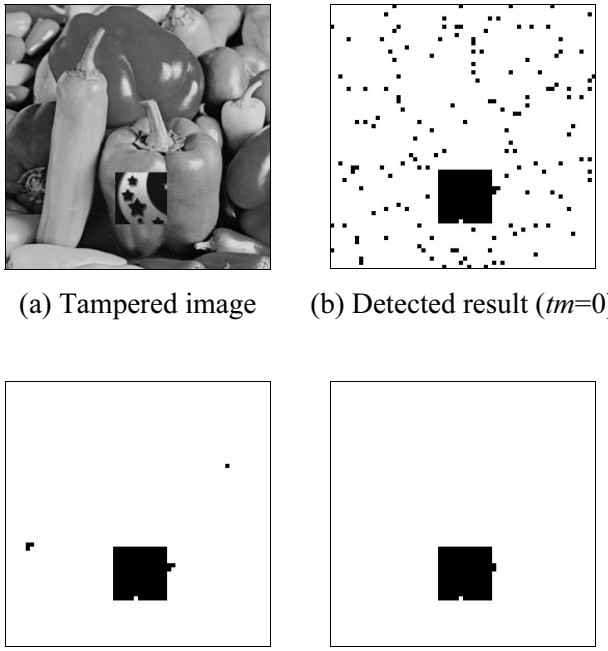


Figure 10. Detected blocks under distinct thresholds *tm*



(a) Tampered image (b) Detected result (*tm*=0)

(c) Detected result (tm=2) (d) Detected result (tm=3)

Figure 11. Visual detection results under distinct thresholds *tm*

Table 1 and Table 2 display results of the previous scheme [12] proposed by Wu and Lin and our scheme, respectively, for five test images under 50 × 50 tampering tests. The results explicitly show that the quality of our authenticated image reached as high as 52dB on the average and it is also superior to those produced by Wu and Lin's scheme [12]. That is the reason that the embedding of authentication data was only executed on 1-LSB bit of each pixel and there were eight pixel values not been modified among every four blocks. These images to be authenticated were subsequently modified by a single small attack of 50 × 50 size in order to simulate the illegal modifies over public networks. Our scheme is able to recover these images having good visual qualities of the recovered images that almost reached 35dB on the average, whereas the previous scheme [12] failed to recover the image. That is because the extent of tampering regions exceeds the tolerant bound of QR error correction. As a result, the extracted QR codes is unreadable such that the scheme [12] cannot detect and recover the tampered areas.

Table 1. Results of the previous scheme [12] for images under 50 × 50 tampering tests

Images	Authenticated image	Tampered image	Recovered image
Barbara	51.14	20.14	38.32
Lena	51.11	21.66	N/A
Pepper	51.09	20.81	N/A
Sailboat	51.01	22.20	N/A
Toys	50.96	20.96	N/A
Average	51.06	21.15	N/A

Note. N/A means that image is not available

Table 2. Results of the proposed scheme for images under 50 × 50 tampering tests

Images	Authenticated image	Tampered image	Recovered image
Barbara	52.18	20.24	35.52
Lena	52.10	21.61	37.72
Pepper	52.20	22.00	36.64
Sailboat	51.84	21.81	32.15
Toys	53.39	20.81	32.50
Average	52.34	21.29	34.91

Here, we visually display two of five test results as examples, such as "Lena" and "Pepper" shown in Figure 12 and Figure 13, respectively. Observing the results in Figure 12(c) and Figure 13(c), it is clear that our scheme can detect 50 × 50 tampered blocks and recover them roughly to that almost similar to the original state. In Figure 13, the result of recovered image has a little of restoring inaccuracy. The reason is that the modified block was much larger than error correction bound, such that Reed-Solomon decoder cannot correct some symbol errors. Here we use RS(15, 9) code, where m =4, n=15, k=9, and t=3; in other words, that encoder of 15 symbols with 9 data symbols can correct up to 3 erroneous symbols. In general, the higher the value of t is, the better the error correction

capability but the more the redundant parity symbols will be. It would result in producing the degrading quality of the authenticated image.

(a) Authenticated image (b) Tampered image

(c) Detected result (d) Recovered image

Figure 12. Visual results for the image "Lena"

(a) Authenticated image (b) Tampered image

(c) Detected result (d) Recovered image

Figure 13. Visual results for the image "Pepper"

In order to show the error correction capability of Reed-Solomon code, the recovered images of our scheme under distinct tampering tests including some regular $N \times N$ regions and an irregular region are presented in Figure 14. It is obviously seen that our scheme can exactly repair modifications when the tampering regions are less than 30×30 size. Moreover, the qualities of recovered images are also over 50dB. As for a test of an irregular region, in addition, we tried to modify a human face of image "Lena" as shown in Figure 14(g). And Figure 14(h) is the corresponding repaired image. Due to that the modified region was too large, there are still bitty blocks not be repaired. But, the contour of human face for image "Lena" have been repaired roughly.

(a) Tampered image, 29.89dB, of a 30×30 region (b) Recovered image, 50.51dB, of (a)

(c) Tampered image, 33.26dB, of a 20×20 region (d) Recovered image, 50.81dB, of (c)

(e) Tampered image, 39.03dB, of a 10×10 region (f) Recovered image, 51.06dB, of (e)

(g) Tampered image, 27.84dB, of an irregular region (h) Recovered image, 35.78dB, of (g)

Figure 14. Recovered image quality under distinct tampering tests

5 Conclusions

This paper proposed a block-wise authentication scheme by using the vector indexing. We introduced error-correcting RS code to protect VQ index result doubly, treating as the authentication and recovery data of image blocks. Once an authenticated blocks was modified, the policy of error correction of RS code will be started up to repair the VQ indices. As shown in the experiments, our scheme in both detection and recovery procedures is feasible. Even though we tampered with a larger region in the authenticated image, the rough contour of an original image can still be repaired and be displayed in its recovered image.

Acknowledgments

This research was supported by the Aletheia University, Taiwan, Republic of China, under the Grant AU-AR-105 -009.

References

[1] S. Ababneh, R. Ansari, A. Khokhar, Iterative Compensation Schemes for Multimedia Content Authentication, *Journal of Visual Communication and Image Representation*, Vol. 20, No. 5, pp. 303-311, July, 2009.

[2] F. Ahmed, M. Y. Siyal, V. U. Abbas, A Secure and Robust Hash-based Scheme for Image Authentication, *Signal Processing*, Vol. 90, pp. 1456-1470, May, 2010.

[3] C. S. Chan, An Image Authentication Method by Applying Hamming Code, *Pattern Recognition Letters*, Vol. 32, No. 14, pp. 1679-1690, October, 2011.

[4] J. C. Chuang, Y. C. Hu, C. C. Lo, W. L. Chen, Grayscale Image Tamper Detection and Recovery Based on Vector Quantization, *International Journal of Security and Its Applications*, Vol. 7, No. 6, pp. 209-228, November, 2013.

[5] Y. H. Chen, C. Y. Lin, W. Sirakriengkrai, I. C. Weng, Repairable Image Authentication Scheme, *International Journal of Network Security*, Vol. 17, No. 4, pp. 439-444, July, 2015.

[6] C. H. Chen, Y. L. Tang, W. S. Hsieh, An Image Authentication and Recovery Method Using Optimal Selection of Block Types, *IEEE International Symposium on Multimedia*, pp. 151-154, December, 2014.

[7] C. S. Lu, H. Y. M. Liao, Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme, *IEEE Transactions on Multimedia*, Vol. 5, No. 2, pp. 161-173, June, 2003.

[8] C. Y. Lin, P. Prangjarote, C. H. Yeh, Reversible Joint Fingerprinting and Decryption Based on Side Match Vector Quantization, *Signal Processing*, Vol. 98, pp. 52-61, May, 2014.

[9] S. Walton, Information Authentication for a Slippery New Age, *Dr. Dobb's Journal*, Vol. 20, No. 4, pp. 18-26, April, 1995.

[10] S. B. Wicker, V. K. Bhargava, *An Introduction to Reed-Solomon Codes and Their Applications*, IEEE Press, 1994.

[11] W. C. Wu, H. F. Hsu, Apply Reed-Solomon Code to Image Authentication, *Proceedings of the 2016 Cryptology and Information Security Conference*, Taichung Taiwan, 2016, pp. 19-23.

[12] W. C. Wu, Z. W. Lin, SVD-Based Self- Embedding Image Authentication Scheme Using Quick Response Code Features, *Journal of Visual Communication and Image Representation*, Vol. 38, No. 7, pp. 18-28, July, 2016.

[13] P. W. Wong, N. Memon, Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification, *IEEE Transactions on Image Processing*, Vol. 10, No. 10, pp. 1593-1601, October, 2001.

[14] S. S. Wang, S. L. Tsai, Automatic Image Authentication and Recovery Using Fractal Code, *Pattern Recognition*, Vol. 41, No. 2, pp. 701-712, February, 2008.

[15] C. W. Yang, J. J. Shen, Recover the Tampered Image Based on VQ Indexing, *Signal Processing*, Vol. 90, No. 1, pp. 331-343, January, 2010.

[16] R. M. Gary, Vector Quantization, *IEEE ASSP Magazine*, Vol. 1, No. 2, pp. 4-29, April, 1984.

[17] P. R. Athira, G. Geethu, K. H. Nithya, M. S. Shima, N. Jumana, A Comparative Study of Image Authentication Techniques in Noisy Channels, *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 5, No. 3, pp. 5356-5362, March, 2017.

[18] H. Zhang, C. Wang, X. Zhou, Fragile Watermarking for Image Authentication Using the Characteristic of SVD, *Algorithms*, Vol. 10, No. 27, pp. 1-12, February, 2017.

[19] C. C. Lin, Y. Huang, W. L. Tai, A Novel Hybrid Image Authentication Scheme Based on Absolute Moment Block Truncation Coding, *Multimedia Tools and Applications*, Vol. 76, No. 1, pp. 463-488, January 2017.

[20] J. S. Lee, C. C. Chang, H. Y. Tsai, A User-Friendly and Authenticationable Secret Image Sharing Scheme, *Journal of Internet Technology*, Vol. 15, No. 3, pp. 433-439, May, 2014.

Biography

Wen-Chuan Wu received the B.S. degree (2001) in Computer Science and Information Engineering from Tung-Hai University, Taichung, Taiwan. Then, she received her M.S. degree (2003) and Ph.D. degree (2007) in Computer Science and Information Engineering from National Chung-Cheng University, Chiayi, Taiwan. Currently, Dr. Wu is an Associate Professor in the Department of Computer Science and Information Engineering (CSIE), Aletheia University, Taipei, Taiwan. Her research interests include image processing, data compression, digital watermarking, information hiding & security, multi-media database retrieval, and Internet of Things.