Pattern Matching Quantization for Image Substantiation

[1]Thrupunoori Varshika, [2]Siri Chandana Tangutoori
[1]Student, [2]Student
Department of electronics and communication engineering, JNTUH college of engineering, Hyderabad, India

Abstract: Image substantiation which provides a means of ensuring the integrity of an image and identify the presence of unauthorized alterations is a systematic way to preserve components of digital images. Pattern Matching Quantization is a classical quantization from signal processing that allows the modelling of probability density functions by the distribution of prototype vectors. It was originally used for data compression. It works by dividing a large set of points (vectors) into groups having approximately the same number of points closest to them. Each group is represented by its centroid point, as in k-means and some other clustering algorithms. A Pattern matching compressed code is not only a remarkable image substantiation feature but also applicable in re-establishing the possibly disfigured pixels. However, if an image is subjected with unauthorizes alterations the required recovery contents vanishes. In order to prevent this difficulty, this paper proposes a quantization-based image substantiation scheme using Matrix barcodes is employed to preserve crucial contents of an image. Matrix barcodes incorporate rectangles, dots, hexagons, and other geometric patterns to form scannable squares and rectangles. This paper presents assimilating pattern matching quantized- code into matrix barcodes and embedding those barcodes into the image itself.

***Key Terms* – Pattern Matching Quantization, Image Substantiation, Matrix Barcode, Quantized Code, Disfigured pixel detection.**

1. INTRODUCTION

Data compression is the mapping of data set into a bit stream to decrease the number of bits required to represent the data set. With data compression, one can store more information in a given storage space and transmit information faster over communication channels. Suppose a source is producing symbols from an alphabet of size 2b at a rate of R symbols per second. Each symbol can be described with an index that is b bits long. Because the rate of the source is Rb bits per second, the data would need to be compressed to be transmitted over channels with capacity less than Rb.

The two types of data compression are lossless and lossy. Lossless compression has the advantage that the original information can be recovered perfectly from the compressed data. In this paper we see Image substantiation which is one of the techniques for protecting the content integrity of digital images from malicious and unauthorized modification. Image substantiation technology can detect and indicate any changes or tampered regions in a disfigured image.

2. PATTERN MATCHING QUANTIZATION CODING

In quantization coding which is a prominent lossy data compression technique that guarantees the achievement of a satisfactory balance between image fidelity and compression ratio. Because of its easy implementation and simple decoding structure, this technique has been widely used in a variety of research fields. The concept of this technique is to replace original image blocks with representative patterns for the purpose of data compression. A Matrix code consists of black and white dots arranged in a square; it also contains special position detection patterns placed in three corners that enable it to be scanned from any direction and still be decoded correctly. The general representation of the matrix code is shown in fig.1.

Fig.1: Representation of Matrix code.

3. QUANTIZATION ENCODING AND DECODING

The generation of the codebook determines the performance of the quantization coding. Pattern matching based quantization coding involves partitioning an image into numerous fixed sized blocks and then comparing them with codewords in the codebook to find the closest pattern for each input vector. On the side of the encoder each of the input blocks is compressed into an index of the codebook. That index is associated with the codebook during the index decoding procedure to rapidly reconstruct the corresponding block through a table lookup operation.

Fig.2: Flow Chart of Pattern Matching Quantization encoding and decoding

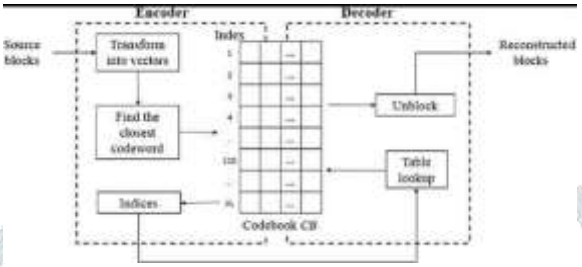
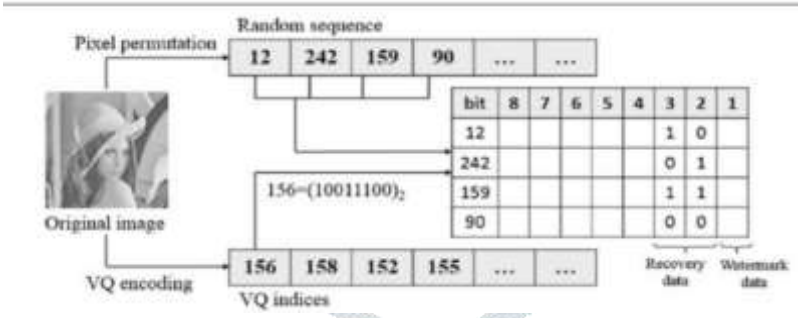


Figure 2 shows the flowchart of pattern matching quantization encoding and decoding. Consider, for example, a grayscale image I of WxH pixels subjected to quantization coding. Initially it is necessary to prepare the code block CB containing Nc representative codewords in which each element $C_i = (c_1^i, c_2^i, \ldots. c_k^i)$ is a k- dimensional vector. Next image I is divided into several non-overlapping blocks with size n x n pixels, where k = n x n, and each image block is then transformed into a vector $X = (x_1, x_2, \ldots\ldots x_n)$.

The image substantiation scheme for re-establishing the disfigured image using pattern matching quantized indexing regards the quantization compressed result, which is the index table, as important recovery information and then embeds it along with substantiation data into the original image. Figure 3 illustrates the flow chart for image substantiation scheme. At the beginning, an image is processed to clear the least significant 3 bits of each pixel into zero.

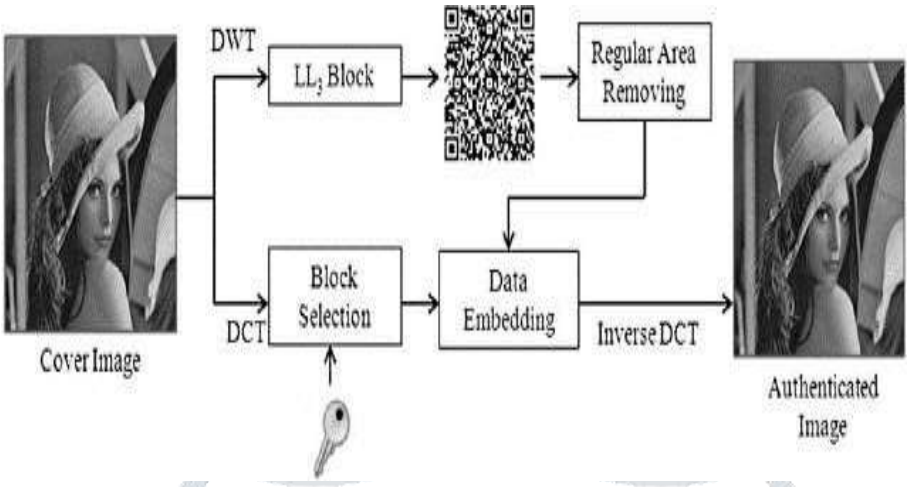
Fig.3: Representation of scheme for image substantiation



Subsequently that result is partitioned into non-overlapping n x n image blocks. Each block is sequentially compressed using a encoder to produce its corresponding quantized index. Because the codeword corresponding to that index is highly similar to the image block in the later recovery procedure. In the tamper detection and recovery procedure, the received authenticated image is verified to determine whether it is genuine or not. The first step is to permute the pixel sequence by using the same random key and then extract three LSBs from each pixel value. The first LSBs are grouped to form an output binary watermark, which is then compared with the original watermark. If the received image is modified in any way, either by changing pixel values or using an inappropriate secret key, then the extracted watermark bitmap becomes incorrect and consequently resembles random noise.

The image tampering detection can be done efficiently by utilizing the properties of data storage and storage error correction of matrix code to secure the substantiation data of an image. A matrix code can hold more data than a traditional barcode can. With the help of error correction, the substantiation data, even when tampered with, can still be completely re-established without error. Figure 4 depicts the flow chart for embedding procedure.

Fig.4: Representation of flow chart for embedded procedure



Initially, an original image is used to perform a discrete wavelet transform to extract a sub-band of the LL_3 block representing a coarse scale of that image. The LL_3 block is then expressed in quantization code format. Using the M error correction level and removing a few regular areas, (such as position detection pattern, alignment pattern, and timing pattern) to generate a small pattern matching code. The remaining areas serve as the substantiation data. The original image is also partitioned into several small and non-overlapping blocks, and a discrete cosine transform (DCT) is performed on each block. This scheme applied a secret key to randomly select block for data embedding. For each chosen block, only five high-frequency DCT coefficients are employed to hide the afore mentioned substantiation data. After the embedding process, these blocks are finally restored to a pixel-domain substantiated image by using an inverse DCT process.

4. PROPOSED SCHEME

To address the problems of the two afore mentioned schemes this section presents the proposed image substantiation scheme for exploiting pattern matched quantization codes to protect the trueness of significant quantization substantiated data generation procedure, and content re-establishment procedure. Before the substantiation data generation procedure is executed, it is necessary to prepare a grayscale image I , called the cover image, with WxH pixels to be authenticated and quantized codebook CB with Nc codewords.

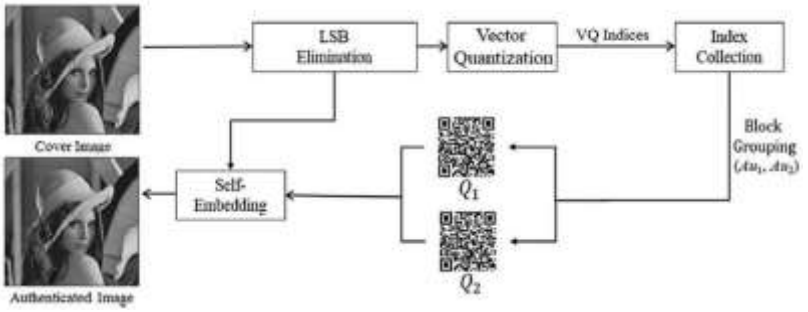
4.1 Substantiation Data Generation Procedure

The purpose of this procedure is to generate substantiation data from the cover image I and then hide them underneath. For clarity, a flowchart of this procedure is presented in figure 5. An LSB elimination operation is first performed to clear the least significant 1 bit (1-LSB) of each pixel to zero for future data embedding. The resulting image I is then encoded using the quantized technique, where each image block is the size of n x n pixels. The encoding result is an index table, consisting of quantized indices, and index idx_i corresponding to the ith image block.

4.2 Image tamper detection procedure

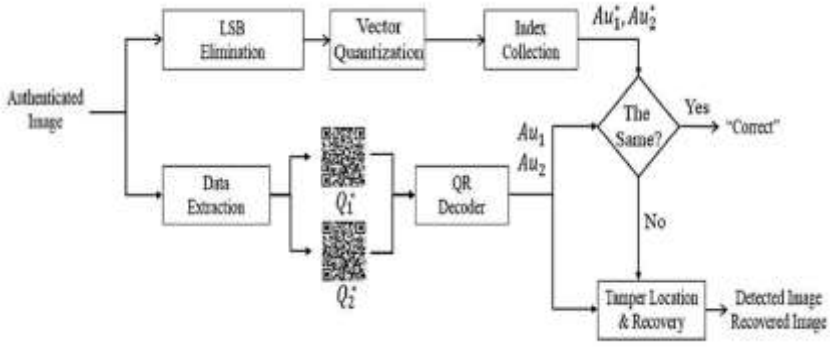
The main purpose of the tamper detection procedure is to accurately detect and mark the suspected modified regions of a substantiated I. Figure 6 shows the flowchart of the tamper detection procedure. The first process entails dividing image I into numerous non-overlapping n x n blocks. These blocks are then scrambled chaotically by using the same sequence RS through key SK. The next process involves extracting the concealed data from the 1-LSB of each pixel and then combining them to form two quantized codes.

Fig.5: Flow chart of data generation procedure



In a detected result, clear blocks are marked in white intensity whereas damaged ones are marked in black intensity. However, not all blocks are able to be detected for content integrity. The main reason is that block grouping operation has been introduced in the prior data generation procedure. Half of quantized indices is recorded only in two quantized codes. Hence, an additional stage is required to detect the other blocks in I more accurately.

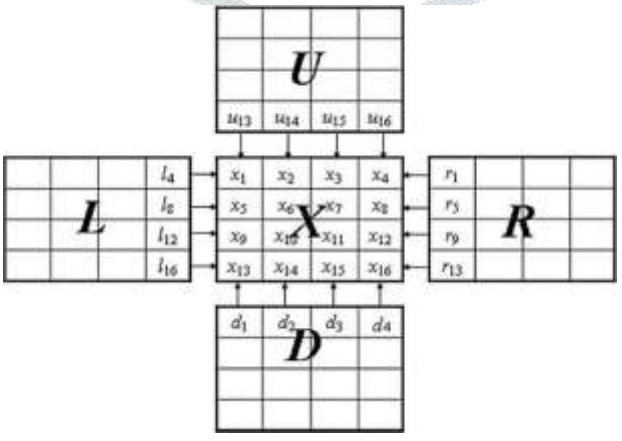
Fig.6: Flow chart for tamper detection



After the detection of tampering procedure, the next process is re-establishment procedure so as to reinstate the image block, especially for the suspected tampered blocks. This procedure mainly aims at the blocks marked black in the prior detected image. Initially, it is necessary to separate detected image into lots of non-overlapping n x n blocks. If an image block is black, it indicates that the block has been modified and it needs to be restored. Such modified blocks are classified into two categories type 1 and type 2. Owing to error correction capability of a quantized code, the encoded data still can be restored completely and lossless even though that code suffered from tolerably damaged. Therefore, we can simply use the corresponding quantized indices to reconstruct the tampered blocks.

The damaged blocks recovery is a bit difficult task and hence a side-match prediction is introduced to reconstruct the blocks approximately. The concept of side-match prediction is shown in figure 7, where the middle block X is what we want to restore and its four adjacent blocks on top, bottom, right, and left directions are U, D, R, and L, respectively.

Fig.7: A diagram for side match prediction

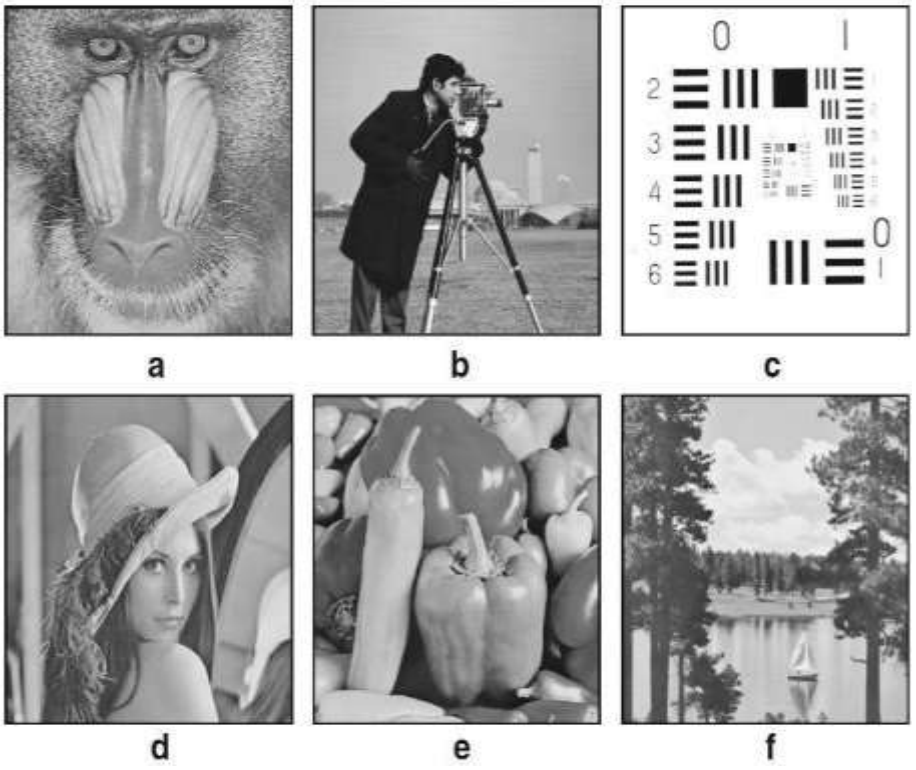


Among them, pixel values in blocks U, D, R, and L, respectively are clear or have been reconstructed already. Due to the image characteristic that neighboring pixels have extremely similar values, the prediction technique is considerably able to recover image content. It is evident that the predicted pixels are inexact and injured, but they are very similar to the original values in general. This way is merely unsuitable to the situation of larger tampering regions. This scheme is necessary to repeat the two steps as mentioned until all the tampered blocks are reconstructed and recovered image being obtained eventually.

5. EXPERIMENTAL RESULTS

As discussed in our experiments, six grayscale images were served as test images, which are shown in figure 10. Each image was performed on LSB elimination and pattern matching quantization operations in order to generate its index table of indices. Then, we took indices from those authentication code to create two quantized codes where an error correction level is L. Afterward, our proposed scheme embeds two quantized codes into the 1-LSB bits of that image. In order to evaluate the qualities of substantiated, tampered, and recovered images, here peak signal to noise ratio is adopted in the experiments.

Fig.8: Six 256 × 256-pixel test images. a. Baboon, b. Cameraman, c. Chart, d. Lena, e. Pepper, f. Sailboat



6. CONCLUSION

In this paper we proposed a simple and effective image substantiation scheme base on pattern matching quantization coding technique. It aims to extract pattern matched quantization compressed code as the substantiation and recovery data of an image and then convert them into matrix quantized code formats. With the capability of error correction and tolerance that matrix codes have, the important confidential data can be protected completely and also without error.

REFERENCES

[1] C.M. Wu, Y.C. Hu, K.Y.Liu, J.C. Chuang, A novel active image authentication scheme for block truncation coding. Image Process Pattern Recognit(2014).
[2] S. Amtullah, A. Koul,Passive image forensic method to detect copy move forgery in digital images (2014).
[3] KH. Pandya, H.J. Galiyawala, Asurvey on QRcodesin context of research and application. Int.J. Emerg.(2014)
[4] S.Jothimani, P.Betty, A survey on image authentication techniques. Int.J.Trends Technol 184-186(2014)
[5] "Information Technology—Automatic Identification and Data Capture Techniques—Data Matrix Bar Code Symbology Specification, ISO/IEC Standard 16022:2006", 2006.
[6] T. V. Bui, N. K. Vu, T. T. P. Nguyen, I. Echizen and T. D. Nguyen, "Robust message hiding for QR code", Proc. IEEE 10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP), pp. 520-523, Aug. 2014