Digital Watermarking On Sparse Based Compressed Fingerprint Images

Nisha Elsa Varghese¹, Nissy Mariam Varghese²

¹Assistant Professor, Department of CSE, St. Thomas college of engineering & Technology Chengannur
²M.sc computer science

Abstract— Fingerprint images have been used as an important biometric recognition technology for image forensics and access control. Due to the increase in the amount of fingerprints collected day by day for a variety of applications, compressing the fingerprint images becomes an emerging technique. In order to enhance the authenticity of fingerprints for investigations, watermarking the compressed fingerprint images will enhance data security. So a novel technique for watermarking on sparse based compressed fingerprint images have been proposed. In this technique, spatial domain of watermarking on compressed fingerprint images is done. A secret key is used to embed and extract watermark. The experimental results show that the peak signal to noise ratio is high after watermarking on compressed fingerprint images. The algorithms are coded and tested by using Matlab2012Rb.

Index Terms-Compression, Fingerprint, k-svd, sparse representation, watermarking, PSNR.

I. INTRODUCTION

Fingerprints are the ridge and furrow patterns on the tip of the finger and are used for personal identification of the people [1]. Federal Bureau of Investigation (FBI) deals with a massive collection of fingerprint cards, which contains more than 200 million cards and is growing at a rate of 30,000 - 50,000 new cards per day [2]. FBI is digitizing these cards to allow for electronic storage, retrieval, and transmission. Fingerprint image compression is a solution to this problem. Generally, compression technologies can be classed into lossless and lossy. Lossless compression allows the exact original images to be reconstructed from the compressed data. While lossy compression technologies usually transform an image into another domain, quantize and encode its coefficients. Two most common options of transformation are the Discrete Cosine Transform (DCT) [3] and the Discrete Wavelet Transform (DWT) [4]. Targeted at fingerprint images, there are special compression algorithms. The most common is Wavelet Scalar Quantization (WSQ). It became the FBI standard for the compression of 500 dpi fingerprint images [5]. These algorithms have a common shortcoming, namely, without the ability of learning. The fingerprint images can’t be compressed well now. So a novel method based on sparse representation for compressing fingerprint images has been proposed[6].

Digital watermarking embeds information within a digital work as a part of the media. Since a good watermarking scheme should always be able to deal with some kinds of attacks, studies in the watermarking research area mostly target robust watermarking problems. “We define watermarking as the practice of imperceptibly altering a Work to embed a message about that Work. We define Steganography as the practice of undetectable altering a Work to embed a secret message” [7]. On the other hand, if get compared with watermarking, encryption is the transformation of data into a secret code with the purpose of protecting the secrecy of the data when sent through an insecure channel; whereas watermarking is the process whereby a host media is embedded with data for the purpose of protection and authentication [8].

For a watermark to be effective, it should satisfy the following features as given in [9]. They are:
Imperceptibility - It should be perceptually invisible so that data quality is not degraded and attackers are prevented from finding and deleting it. A watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, un watermarked content.

Readily Extractable - The data owner or an independent control authority should easily extract it.

Unambiguous - The watermark retrieval should unambiguously identify the data owner.

Robustness – It should tolerate some of the common image processing attacks. A watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copyright protection applications to carry copy and access control information.

The rest of the paper is organized as follows. In Section II, we describe the model of the system. The watermark embedding and decoding process are introduced in Section III. Section IV analyzes and evaluates the performance of the proposed scheme. Experimental results are demonstrated in Section V, and Section VI concludes the paper.

II. WATERMARKING TECHNIQUE AND SPARSE BASED COMPRESSION ON FINGERPRINT IMAGES

The digital watermarking as in [7] involves two major operations: (i) watermark embedding, and (ii) watermark extraction. For both operations a secret key is needed to secure the watermark. The keys in watermarking algorithms can apply the cryptographic mechanisms to provide more secure services. The secret message embedded as watermark can almost be anything, for example, a bit string, serial number, plain text, image, etc. The most important properties of any digital watermarking technique are: robustness, security, imperceptibility, complexity, and verification. Watermarking techniques can be classified according to the nature of data (text, image, audio or video), or according to the working domain (spatial or frequency), or classified according to the human perception (robust or fragile). In images, the watermarking techniques can broadly be classified into three types: (i) visible watermark, (ii) invisible fragile watermark and (iii) invisible robust watermark.

2.1. Spatial and frequency domain watermarking

Watermark usually embeds into either spatial or frequency domain of the media. Spatial domain embedding is a linear operation which deals directly with the host media bytes one by one consequently. Frequency domain embedding is a nonlinear operation that deals confidently with the frequency components of the host media; therefore a transform method needs to be applied [7].

2.2 Compression of fingerprint

A novel method based on sparse representation for compressing fingerprint images is used as in[6].The specific process is as follows: construct a base matrix whose columns represent features of the fingerprint images, referring the matrix dictionary whose columns are called atoms; for a given whole fingerprint, divide it into small blocks called patches whose number of pixels are equal to the dimension of the atoms; use the method of sparse representation to obtain the coefficients; then, quantize the coefficients; last, encode the coefficients and other related information using lossless coding methods.

2.2.1 The Model of Sparse Representation

The model of sparse representation for compressing fingerprint images is given in [6] which is illustrated as follows.
Given $A = [a1, a2, \ldots, aN] \in \mathbb{R}^{M \times N}$, any new sample $y \in \mathbb{R}^{M \times 1}$, is assumed to be represented as a linear combination of few columns from the dictionary $A$, as shown in formula (1). This is the only prior knowledge about the dictionary in our algorithm. This property can be ensured by constructing the dictionary properly.

$$y = Ax \quad (1)$$

where $y \in \mathbb{R}^{M \times 1}$, $A \in \mathbb{R}^{M \times N}$ and $x = [x1, x2, \ldots, xN]^T \in \mathbb{R}^{N \times 1}$.

Obviously, the system $y = Ax$ is underdetermined when $M < N$. Therefore, its solution is not unique. According to the assumption, the representation is sparse. A proper solution can be obtained by solving the following optimization problem:

$$\text{(l0)} : \min \|x\|_0 \text{ s.t. } Ax = y \quad (2)$$

Solution of the optimization problem is expected to be very sparse, namely, $\|x\|_0 < N$. The notation $\|x\|_0$ counts the nonzero entries in $x$. Actually it is not a norm. However, without ambiguity, we still call it $l0$-norm.

In fact, the compression of $y$ can be achieved by compressing $x$. First, record the locations of its nonzero entries and their magnitudes. Second, quantize and encode the records.

### 2.2.2. Dictionary Construction

The dictionary is constructed using a training method called K-SVD [10], [11]. The dictionary is obtained by iteratively solving an optimization problem (3). $Y$ is consisted of the training patches, $A$ is the dictionary, $X$ are the coefficients and $Xi$ is the $i^{th}$ column of $X$. In the sparse solving stage, we compute the coefficients matrix $X$ using MP method, which guarantees that the coefficient vector $Xi$ has no more than $T$ non-zero elements. Then, update each dictionary element based on the singular value decomposition (SVD).

$$\text{Min } \|Y - AX\|_F \quad ; \quad \text{s.t. } \forall i, \|Xi\|_0 < T \quad (3)$$

### 2.2.3. Coding and quantization

Entropy coding of the atom number of each patch of fingerprint images in the dictionary is done by static arithmetic coders [12]. The quantization of coefficients after entropy coding of fingerprint image is performed using the Lloyd algorithm [13].

### 2.2.4 Algorithm 1: Fingerprint compression based on sparse Representation[6]

1. For a given fingerprint, slice it into small patches.
2. For each patch, its mean is calculated and subtracted from the path.
3. For each patch, solve l0-minimization problem by MP method.
4. Those coefficients whose absolute value are less than a given threshold are treated as zero. Record the remaining coefficients and their locations.
5. Encode the atom number of each patch, the mean value of each patch, and the indexes; quantize and encode the coefficients.
6. Output the compressed stream.

The input fingerprint image, dictionary constructed after k-svd on fingerprint image and compressed fingerprint image is as shown in figure1 below.

![Figure 1 (a).input fingerprint image](image1)

![Figure 1 (b).Dictionary constructed](image2)

![Figure 1 (c).Compressed fingerprint image](image3)

The input image is of size 410.6780 KBytes while the compressed fingerprint image (output image) is of size 162.5000Kbytes.

### III. EMBEDDING ALGORITHM FOR WATERMARKING

Three tasks are done by the embedding algorithm[7]: generates extraction key, determines the position of the embedding watermark and then embeds watermark. First of all, the algorithm must determine where the watermark should be located; therefore, a base image(compressed fingerprint image) is divided into 64 blocks. Each block size is: \( \frac{M}{8} \times \frac{N}{8} \) where M and N are the number of the rows and columns of the base image respectively. So there will be eight groups of rows as well as for columns.

The watermark will embed through one of these groups either rows or columns in each base image but randomly for sequence base images.In the selected group a LSB (least significant bit) over all pixels will extract (LSB 0).Then MSB of mark image is extracted.Then MSB of mark is inserted into the LSB of the base image[15].

#### 3.1 Extraction Algorithm

To extract the watermark, the algorithm needs to decrypt extraction key to obtain the initial key, through which the algorithm can locate the watermark position in the targeted base-image. Algorithm needs to divide marked-image to 64 blocks, and then determining the watermark location. The extraction operation begins from the 1st block of the determined group by extracting the LSB from each pixel in the group, and then is multiplied by the ordering number of the block before adding it to the corresponding pixel in the zero-image (by this step all pixels LSB will become valued not default Zero). This will be repeated eight times to revalue the zero-images pixels with watermark real values obtained from the marked-image LSBs, and the result will be the watermarked image.
3.2 Steps for watermarking.

1. Read Watermark Image and key to encrypt image.
2. Read Base Image-sparse based compressed fingerprint image.[16]
4. Divide Base Image (8 X 8).
5. Determine the Watermarking Location:
6. Embed Watermark into Base Image and perform bitwise X-OR operation with the key and watermarked image.
7. Result is: Invisible Watermark.
8. To de watermark the image, first the watermarked image is bitwise X-OR ed with the key and finally we can extract the image.

The base image is sparse based compressed fingerprint image. The mark image is embedded into base image to get marked image. Finally we can extract the mark image.

IV. EXPERIMENTAL RESULTS

4.1 Results

Numerical experiments are performed on three databases namely, Database-1, Database-2, Database-3 which can be downloaded from[14]. The size of the fingerprints in the database is 640 X 640[1]. The mark image is ‘w.jpg’. This image can be used to enhance security of fingerprint image. If the key is correct, then only the receiver can decrypt the image. the watermarking technique is shown in figure 2 below:

![Watermarking on compressed fingerprint image](image)

Figure 2: Watermarking on compressed fingerprint image

4.2 Performance Evaluation

The quality measure used to analyze quality of watermarked fingerprint image is PSNR(peak signal to noise ratio). The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed...
image. The higher the PSNR, the better the quality of the compressed, or reconstructed image. From this value we can ensure the output is received with the same or good quality at the receiver side.

$$PSNR = 10 \log_{10} \left( \frac{255^2}{MSE} \right)$$

where MSE is given by,

$$MSE = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{[OI(i, j) - DI(i, j)]^2}{MN}$$

where OI is original image and DI is the distorted image i.e. compressed image.

The PSNR value of watermarked image is 66.5217, which indicates that there is very little deterioration in the quality of original image.

V. CONCLUSION

A novel technique of watermarking on sparse based compressed fingerprint images has been proposed. In order to enhance the authenticity of fingerprints for investigations, watermarking the compressed fingerprint images will enhance data security. In this technique, spatial domain of watermarking on compressed fingerprint images is done. A secret key is used to embed and extract watermark. The experimental results show that the peak signal to noise ratio is high after watermarking on compressed fingerprint images. As a future work, the optimization algorithms for solving the sparse representation need to be investigated. Also watermarking in frequency domain can also be done.

REFERENCES


