ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Watermarking of the Fingerprint Template using Optimal Frequency Band

Amanpreet Kaur Wadhwa[1], Monica Goyal[2]

Guru Gobind Singh College of Engg.,& Technology, Guru Kashi University, Talwandi Sabo, Bathinda, Punjab, India[1,2]

Abstract: Fingerprint is the most appreciated biometric identification system in the world today. The latest technology of the fingerprint identification has made the identification and verification of the human beings easy. But the database of the fingerprint templates is still unprotected except physical security. On the other hand invisible watermarking has enhanced the security in images. My topic is a combined approach for the security and image quality preservation of the fingerprint template images which are stored inside the database for future reference. The templates are watermarked with invisible logo, which is checked before the minutiae extraction process of the verification process. If the invisible watermark is missing or distorted then the template is considered to be a bogus or tampered one and the identification process fails.

Keywords: Discreet Cosine Transform (DCT), Watermarking, Fingerprint Template, Invisible Watermark, Frequency Distribution, Spatial Domain.

I. INTRODUCTION

A fingerprint is the feature pattern of one finger[1]. It is believed with strong evidences that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have being used for identification and forensic investigation for a long time [2].

Fig. 1 A fingerprint image acquired by an Optical Sensor

A fingerprint is a pattern of ridges and furrows which have average width and are parallel aligned to each other[4].

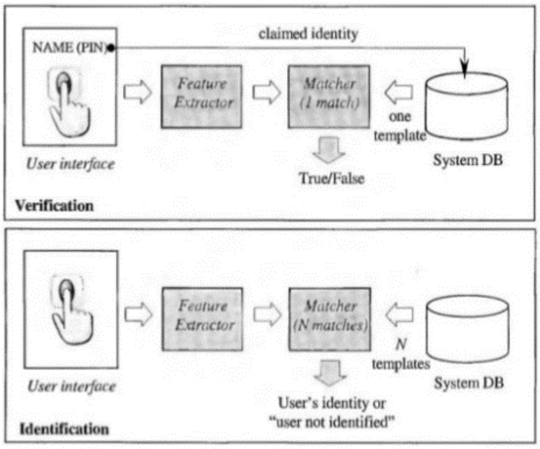


Fig 2. Fingerprint Identification vs. Fingerprint Verification

The fingerprint recognition can be divided into two categories: one is fingerprint verification and the other is fingerprint identification[3]. Fingerprint verification is to verify the authentication of one person using his fingerprint[9]. The fingerprint verification system retrieves the fingerprint template image and matches the template image with the real-time captured fingerprint through the user.

On the other side, all fingerprint recognition scenarios, either fingerprint verification or identification are based on a fingerprint template. The fingerprint matching, for the 1-to-1 verification case or 1-to-m identification case, is straightforward and easy.

II. THE WATERMARKS

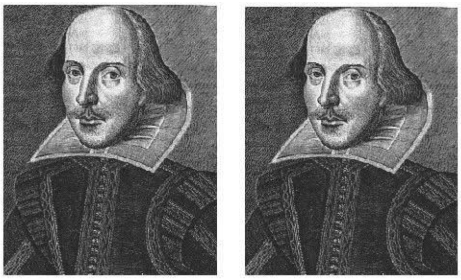


Figure 3. Non watermarked name (Left) and Invisible Watermarked Image (Right)

A watermark is an identifying feature, like a logo, which can be used to provide protection of some "cover" data. [10] A watermark may be either visible i.e. perceptible, or invisible i.e. imperceptible. Or any piece of data may be used as a watermark. The most common watermarks used include company logo, number sequences, and also watermarks consisting of black and white dots. A watermark is a pattern of bits inserted into a digital image file that identifies the file's copyright information (author, rights, etc.). The name ―watermark is derived from the faintly visible marks imprinted on image. Unlike printed watermarks, which are intended to be somewhat visible or totally invisible, in our work the effort is made specifically to design completely invisible watermark. Satisfying all these requirements is no easy, but there are a number of researchers that have proposed the techniques for the digital watermarking. All of them work by making the watermark appear as noise - that is, random data that exists in most digital files which needs to be reduced as much possible.

III. Types of Watermark

There are two well-known approaches to watermarking that are:

A. Spatial Domain Watermarking

Spatial domain watermarking[6] is one which do not requires original image for watermark detection. However, it often fails under signal processing attacks such as filtering and compression[4]. Besides, the fidelity of the original image data can be severely degraded since the watermark is directly applied on the pixel values[6].

B. Transform Domain Watermarking

Title Watermark embedded in the transform domain e.g., DCT, DFT, wavelet by modifying the coefficients of global or block transform[7]. Frequency domain watermarking generally provides more protection under most of the signal processing attacks. But the existing frequency-domain watermark algorithms require the original image for comparison in the watermark retrieval process, which is not practical for a huge image database. Furthermore, the necessity of progressive transmission is one of the requirements for Internet distribution. The lack of progressive transmission property in existing spatial- and frequency-domain watermarking[7] algorithms limits their Internet applications.

The basic advantage of using the transform domain watermarking is that we have more control over the watermark insertion areas that are basically the areas of interest for inserting the watermark because in transform domain watermarking we have more than one coefficients against every pixel value.

IV. Using Watermarks in Fingerprint Templates

Digital watermarks can be considered data protection technique. A fingerprint template stored in the database can be altered to gain fake authentication. The approaches are valid for utilizing watermarks immediately for copy protection using devices for watermarking at template recording time[9].

Protection can occur at two separate stages, during recording and reusing of the fingerprint image. In each case both the presence of a potentially specific watermarking or the absence of watermark can be used to detect genuinely. Requiring the presence of a watermark to permit playback of fingerprint template require some similarity to the authentication system. Depending on the robustness requirements for the watermark, watermark recognition may even be possible from copies generated from analog sources.

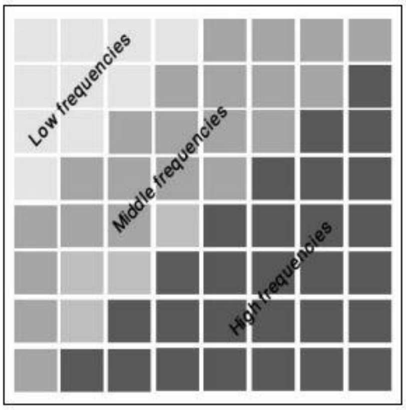


Figure 4. Mid band frequencies of the image.

The image is the 2 dimensional representation of the pixels. The pixels of the standard image can be converted to coefficients after the application of discreet cosine transform (DCT). The DCT image coefficients are separated into Low, Middle and High Frequencies. The low and High frequency pixels if altered, adds to distortion and reduces the Peak Signal To Noise Ratio (PSNR)[18] which indicates the poor quality of the image.

In this chapter, a detailed overview of the proposed method is represented. The fingerprint templates are the pattern of ridges and furrows[5]. From each fingerprint image, many minutiae i.e. unique points are extracted at the time of matching one fingerprint to other or for matching a fingerprint to a database of the fingerprints [17]. For the higher security, an invisible watermark is embedded to the fingerprint template which does not affect the template quality.

The embedding of the watermark is done with the help of Discreet Cosine Transform (DCT) along with basic Least Significant Bits (LSB)[13] technique. The technique uses the middle band of the fingerprint template image for selection of potential locations by using DCT coefficients[15].

In basic Least Significant Bit technique, the bits from secret image simply overwrite LSBs, i.e. Maximum four least significant bits of the fingerprint template image, while low band and high bands remain unchanged. Embedding data in higher bit planes may sometime results in quality artifacts in the template image.

In my work, I have attempted to embed logo image into middle frequency blocks as the middle avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks whereas higher frequency blocks provide better image quality which enhances the output image and reduces noise to great extent[14].

The Discrete Cosine Transform (DCT)[8] firstly divides the image into pixel wise intensity map and then transforms the image from spatial domain to frequency domain. Also, it separates the image into spectral sub-bands with respect to its visual quality, i.e. high, middle and low frequency components[12].

DOI 10.17148/IJARCCE.2015.48104

The watermark is embedded in the coefficients of fingerprint template to avoid visual distortion.

The proposed method is used to hide a secret object (text, image or logo) into the fingerprint template. As shown in figure 1, the method depends on transforming the cover image from spatial to frequency domain, and convert the secret object into a bit sequence[11]. The embedding process watermark bit sequence in the specified band in the frequency domain media using LSB on coefficients in order to get a safe area to hide watermark invisibly[16]. DCT helps in uniform quantization of the template[9].

ALGORITHM

The proposed algorithm for Invisible Watermark insertion in fingerprint template:

Step 1: Load the fingerprint template image.
Step 2: Load the Watermark Image.
Step 3: Apply DCT to divide cover image blocks and decompose to the frequency bands
Step 4: Convert the Watermark to bit sequence.
Step 5: Replace the LSB of the middle band blocks of the fingerprint template with the watermark bit sequence according to the selected pixel intensity.
Step 6: Reconstruct the fingerprint template.
Step 7: Save the template to the database.

A. *Performance Metrics*

1: Normalized Absolute Error (NAE)

It’s the numerical difference between the two images i.e. the original and new image formed. Where i = 1 to m and j = 1 to n. Also the A and B are the image approximations used for calculations. NAE [19] can be represented as:

$$\mathrm{NAE} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(|A_{ij} - B_{ij}|)}{\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{ij})}$$

2: Average Difference (AD)

Average Difference[19] denotes the average of the difference between the pixels of the original and the treconstructed image. The lesser the AD, better is the image. Average Difference (AD) can be represented as:

$$AD = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j) - y(i,j))$$

3: Peak Signal To Noise Ratio (PSNR)

Peak signal to noise ratio (PSNR)[19] which is defined as the maximum signal of the image to the noise ratio. More the noise, lesser is the PSNR. PSNR is measured in db (decibels).

$$\mathrm{PSNR} = 10\log_{10}\frac{(\mathrm{L}-1)^2}{\mathrm{RMS}}$$

Where

$$\mathrm{RMS} = \frac{1}{\mathrm{m}\cdot\mathrm{n}}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(\mathrm{x}_{i,j} - \mathrm{x}'_{i,j}\right)^2$$

4: Mean Square Error(MSE)

Mean Square Error[19] is defined as any measure of the *center* of a distribution that is associated with measure of *error*. We measure the quality of *t*, as a measure of the center of the distribution, in terms of the *mean square error*.

$$\mathrm{MSE}(t) = \frac{1}{n}\sum_{i=1}^{k} f_i (x_i - t)^2 = \sum_{i=1}^{k} p_i (x_i - t)^2$$

MSE (*t*) is a weighted average of the squares of the distances between *t* and the class marks with the relative frequencies as the weight factors.
The mean square error (MSE) is used to find difference between an estimation and original value. MSE measures the average of the square of the "error," with the error being the amount by which the estimator differs from the quantity to be estimated.

B. *Results*

Fingerprint Image no. 101_6

Image	PSNR	MSE	NAE	AD
101_6	39.0864	0.074075	0.0095	-0.0003

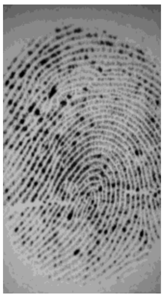
Fingerprint Image no. 102_4

Image	PSNR	MSE	NAE	AD
102_4	39.4893	0.074053	0.0075	-0.0001

DOI 10.17148/IJARCCE.2015.48104

Fingerprint Image no. 104_3

Image	PSNR	MSE	NAE	AD
104_3	39.4887	0.740638	0.0070	0.0000



Fingerprint Image no. 107_1

Image	PSNR	MSE	NAE	AD
107_1	39.2678	0.0740396	0.0065	-0.0002

Fingerprint Image no. 108_8

Image	PSNR	MSE	NAE	AD
108_8	39.2664	0.0740638	0.0059	0.0000

Fingerprint Image no. 104_6

Image	PSNR	MSE	NAE	AD
104_6	39.1302	0.0740638	0.0076	0.0000

Fingerprint Image no. 103_7

Image	PSNR	MSE	NAE	AD
103_7	39.6626	0.0740638	0.0061	0.0000

V. CONCLUSION

The conclusion of my work states that the fingerprint watermarking acts as an effective measure to protect the database templates. The selection of the random allocation of the watermark in the fingerprint template helps to preserve the image quality. Moreover the invisible watermark insertion inside the fingerprint template leads to the increased security of the templates. Any tempered or the digitally altered fingerprint template could not get selected as the database template with hacking of the database. The mid band DCT method allows to store the watermark invisibly which affects negligibly the quality of the fingerprint image.

REFERENCES

[1] Ameya K. Nail, Raghunath S. Holambe.” A blind DCT domain digital watermarking for biometric authentication.” International Journal of Computer Applications (0975-8887) VOL. 1, NO. 16, 2010, pp. 11-15.

[2] Anil K. Jain, UmutUludag. “Hiding Biometric Data.” IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 25, NO. 11, NOVEMBER 2003: 1494-1498.

[3] Dipesh Agrawal, SamidhaDiwedi Sharma. “Analysis of Random Bit Image Steganography Techniques.” International Journal of Computer Applications (0975 – 8887) International Conference on Recent Trends in engineering & Technology - 2013(ICRTET'2013).

[4] Hardik Patel, Preeti Dave. “Steganography Technique Based on DCT Coefficients.” International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 1, Jan-Feb 2012, pp.713-717.

[5] Heeseung Choi, Kyoungtaek Choi, Jaihie Kim. “Fingerprint Matching Incorporating Ridge Features with Minutiae. ”IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011: 338-345.

[6] Inderjit Singh, Sunil Khullar2, Dr. S.C. Laroiya. “DFT Based Image Enhancement and Steganography” International Journal of Computer Science and Communication Engineering (ISSN: 2319-7080), Volume 2, Issue 1, February 2013: 5-7.

[7] K. Naveen BrahmaTeja, Dr.G. L. Madhumati, K. Rama Koteswara Rao. “Data Hiding Using EDGE Based Steganography.” International Journal of Emerging Technology and Advanced Engineering (IJETAE) ISSN 2250-2459, Volume 2, Issue 11, November 2012: 285-290.

DOI 10.17148/IJARCCE.2015.48104

[8] Dr. K. Ramanjaneyulu, Dr. P. Pandarinath, B. Rakesh Reddy. "Robust and Oblivious Watermarking based on Swapping of DCT Coefficients." International Journal of Application or Innovation in Engineering & Management (IJAIEM). ISSN 2319 – 4847, Volume 2, Issue 7, July 2013.

[9] K.Saranya, Dr.C.SureshGnanadhas, MinuGeorge." Data Embedding Techniques in Steganography." International Journal of Latest Trends in Engineering and Technology (IJLTET). ISSN: 2278-621X, Vol. 3 Issue2 November 2013, pp. 200-205.

[10] Kaiser J. Giri, Mushtaq Ahmad Peer, P. Nagabhushan. "A Robust Color Image Watermarking Scheme Using Discrete Wavelet Transformation."International Journal of Image, Graphics and Signal Processing (IJIGSP) 7, no. 1 (2014): 47-52.

[11] Kaushal Solanki, Noah Jacobsen,UpamanyuMadhow, B. S. Manjunath,ShivkumarChandrasekaran. "Robust Image-Adaptive Data Hiding Using Erasure and Error Correction." IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 13, NO. 12, DECEMBER 2004: 1627-1639.

[12] LahouriGhouti, Ahmed Bouridane, Mohammad K. Ibrahim, Said Bousakta." Digital Image Watermarking Using Enhanced Multiwavelets". IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 54, NO. 4, APRIL 2006: 1519-1536.

[13] MasoudNosrati, Mehdi Hariri, RonakKarimi. "An introduction to steganography methods." World Applied Programming, vol. 1, no. 3, AUGUST 2011: 191-195.

[14] Mohammad Tafaghodi, MeysamGhaffari, AlimohammadLatif, SeyedRasoulMousavi. "Improving image watermarking based on Tabu search by Chaos." arXiv preprint arXiv: 1501.01576 (2015).

[15] NehaNarula, Deepak Sethi, ParthaPratim Bhattacharya. "Comparative Analysis of DWT and DWT-SVD Watermarking Techniques in RGB Images." International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 8, No. 4 (2015), pp. 339-348 http://dx.doi.org/10.14257/ijsip.2015.8.4.29.

[16] Subhayan Roy Moulick, Siddharth Arora, Chirag Jain, Prasanta K. Panigrahi. "Reliable SVD based Semi-blind and Invisible Watermarking Schemes." arXiv preprint arXiv: 1503.01934 (2015).

[17] Vaibhav B. Joshi, Mehul S. Raval, Priti P. Rege, S. K. Parulkar. "A Multiple Reversible Watermarking Technique for Fingerprint Authentication." Multimedia Systems (2015): 1-12.

[18] Vidyasagar M. Potdar, Song Han, Elizabeth Chang. "A survey of digital image watermarking techniques." In Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on, pp. 709-716. IEEE, AUGUST 2005.

[19] Kumar, Ravi, and Munish Rattan. "Analysis of various quality metrics for medical image processing." IJARCSSE 2 (2012): 11-160.

DOI 10.17148/IJARCCE.2015.48104