A Data Hiding Capacity Estimation Technique for Biometric Images

Ghazaleh Sarbishei
Ferdowsi university of Mashad
Gh_sarbishei@gmail.com

Saied Hossaini Khayat
Ferdowsi university of Mashad
shk@alum.wustl.edu

Abstract- In this paper an estimation technique for the data hiding capacity in biometric images is presented. We consider the QSWT algorithm for data hiding in biometric images and investigate the effect of message strength in increasing capacity in the presence of different types of attacks.

Keywords- data hiding, image watermarking, DWT, QSWT, channel capacity.

1- Introduction

Data hiding refers to embedding information within a host data such as text, audio, image or video. In watermarking applications, the hidden data represents authorship information, a time stamp or copyright information [1]. Data hiding in biometric images has been proposed to make the biometric systems secure and resilient to deliberate manipulations and attacks.

Data hiding capacity is a measure of the amount of information that can be hidden in a digital image while satisfying requirements such as robustness and invisibility. Estimating the capacity can set an upper-bound to the amount of data that can be hidden in an image, therefore it can help in the design of efficient data hiding algorithms. There has been ongoing research in data hiding capacity estimation in recent years. In [2], each pixel is considered as an independent channel and the capacity is calculated based on the theory of parallel Gaussian channels. Reference [3] presents an information theoretic model for data hiding and studies the capacity problem under several types of attacks. In [4], zero-error information hiding capacity in JPEG-compressed domain is presented. Reference [5], presents an analysis of watermarking capacity based on the content of wavelet subbands and uses the concept of wavelet quantization matrix and Noise Visibility Function.

The factors determining data hiding capacity include (1) the statistical model used for the host image, (2) the distortion constraints placed on the data hider and the attacker, and (3) the information available to the data hider, attacker and decoder. In fact, the content of an image has great influence on its data hiding capacity. Data hiding capacity can also be influenced by the watermark strength, but high strength does not necessarily imply high capacity, as will be shown in simulation results. In previous works [2-5], capacity is estimated for data hiding in wavelet domain. In those works, the watermark strength is constrained based on the content of wavelet subbands.

In this paper, a framework for estimating the capacity of data hiding in biometric images based on QSWT algorithm is presented. Automated biometrics can provide accurate and reliable user authentication method.

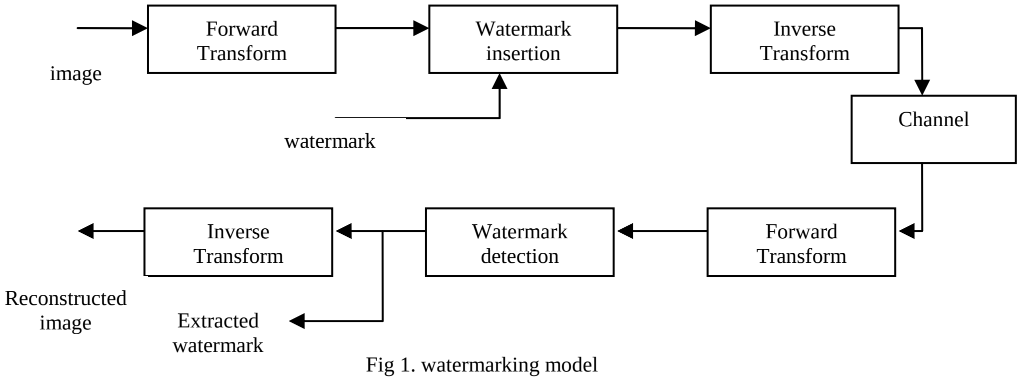


Fig 1. watermarking model

Watermarking biometric images can guarantee secure transmission of acquired images from intelligence agencies to a central image data base [6]. We assume that these watermarked biometric images are used for automatic user recognition and authentication. Since authentication will be done automatically, considerations of Human Visual System in watermarking can be ignored to some extent. In other words, in this proposed scheme, watermark (message) strength can be distributed equally among different wavelet subbands, regardless of their frequency contents.

Also in this paper, we compare the data hiding capacity in the presence of different attacks and discuss the effect of increased watermark strength on the capacity.

This paper is organized as follows. In section 2, a mathematical model used for image watermarking is presented. Section 3 describes the QSWT approach for data hiding. Section 4 gives capacity results for Gaussian channels. In section 5, simulation results for biometric images are presented.

2- Mathematical model for data hiding

In data hiding schemes, a host image is

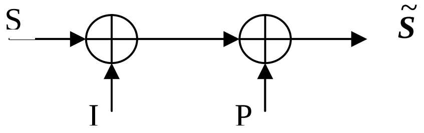


Fig 2. Data hiding channel [9]

considered as a communication channel for transmitting messages.

Therefore, watermarking capacity can be estimated using traditional information theory. Fig. 1 shows a common model for watermarking in transform domain. In this model, the forward transform block decomposes the image into its coefficients of L bands. This forward transform can be either discrete cosine transform (DCT) or discrete wavelet transform (DWT). Then, a watermark (message) is added to each band. The watermarked image is reconstructed using an inverse transform block. This image undergoes some certain type of processing (such as compression, addition of noise, median filtering) to yield the image. At the receiving end, watermark is extracted by decomposing this image into its L bands (using the same forward transform block) and the hidden message is extracted from each band. In this paper, we aim to estimate the capacity of such communication channel which is used to hide messages in biometric images such as fingerprint and iris images. In [9] a model for data hiding channel is presented, as shown in Fig.2 where, S is a watermark (message) to be transmitted through the channel. The channel noise is modeled as a combination of two sources: I the noise due to the host image and P, the noise due to processing. In this paper, we estimate the capacity for the case that image undergoes median filtering, JPEG compression, Gaussian filtering, sharpening and addition of Gaussian noise.

3- Channel Specification

In the above model for data hiding, we assume that the data hiding channel is a combination of L parallel sub-channels. The decomposition of the image is performed by applying a forward DWT transform. DWT transform is identical to a hierarchical subband system where the subbands are logarithmically spaced in frequency domain. The image is first decomposed into 4 parts of high, middle and low frequencies (LL1, HL1, LH1, HH1). The subbands LH1, HL1 and HH1 are the finest scale wavelet coefficients. Subband LL1 is further decomposed and this process is repeated several times. In some data hiding schemes, the watermark message is hidden in these subbands according to the magnitude of their coefficients. So each subband of the wavelet decomposition can be considered as one of the sub-channels defined in our model.

In some schemes, the coefficient selection method is based on the Qualified Significant Wavelet Tree (QSWT) [7]. This method takes the relationships of DWT coefficients and spatial information into consideration and thus achieves more robustness. The principles of QSWT are as follows:

A parent-child relationship can be defined between wavelet coefficients at different scales corresponding to the same location. Excluding the highest frequency subbands, every coefficient at a given scale can be related to a set of coefficients at the next finer scale of similar orientation. The coefficient at the coarse scale is called the *parent*, and all coefficients corresponding to the same spatial location at the finer scales are called *children*. In other words, a family tree is constructed by grouping n levels of wavelet coefficients in the same spatial direction. The parent is a wavelet coefficient in one of the three highest frequency subbands HL$_n$, LH$_n$ or HH$_n$ and its children are the ones located along the same orientation in the next higher scales [8]. For a given parent, the set of all coefficients of all finer scales corresponding to the same orientation are called *descendants*. In Fig. 3 a wavelet tree consisting of all descendants of one coefficient in LH3 is shown.

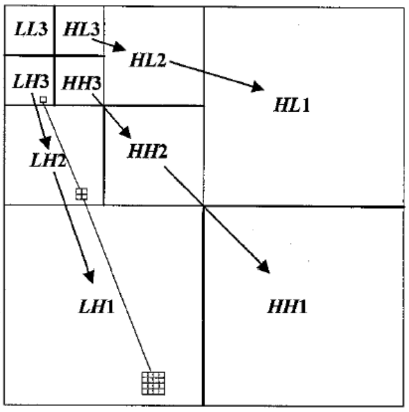


Fig. 3. DWT decomposition and all descendents of one coefficient in LH3.

Choosing an appropriate coefficient as a parent for data hiding is done based on some amplitude thresholds. If a wavelet coefficient $x_n(i,j) \in D$, where D is a subband labeled HL$_n$, LH$_n$, HH$_n$, at the coarsest scale is a parent of $x_{n-1}(p,q)$, satisfying $|x_n(i,j)|\rangle T_1$, $|x_{n-1}(p,q)|\rangle T_2$ and, $p = 2i-1,...,2i,$ $q = 2j-1,...,2j$, $n,i,j\rangle 1$, for a given threshold T_1 and T_2, then $x_n(i,j)$ and its children are called a QSWT [7].

So in this case the elements of each sub-channel are the coefficients of the QSWT.

In this paper, we will show the effect of appropriate data hiding schemes in increasing the data hiding capacity. As will be shown in section 5, we have estimated the data hiding capacity for two cases and compared estimated capacities.

4- Channel capacity

The capacity of an AWGN channel can be calculated according to

$$C = W \log_2 (1 + \sigma_x^2 / \sigma_n^2) \quad (1)$$

in which W is the channel bandwidth , σ_x^2 is the variance of the message signal to be transmitted and σ_n^2 denotes the noise variance . In this work we assume that message is transmitted through L bands of transformed (DWT) image. So in an $M \times N$ pixel image, we have $(M \times N)/L$ coefficients. According to the Nyquist sampling theory, sampling points should be $2W$, so the bandwidth of an image will be $\frac{M \times N}{2L}$ [5].

The decomposition of an image into L subbands results in L parallel sub channels with two noise sources in each sub-channel. Since we have no knowledge about the distribution of these noises, we assume the worst Gaussian distribution [10]; we assume that these two noises are Gaussian and independent. So the channel noise can be replaced by one noise with variance $\sigma_i^2 + \sigma_p^2$ where σ_i^2 is the variance of image noise and σ_p^2 is the variance of processing noise. Thus the total capacity of L parallel channels is given by [9]:

$$C = \frac{MN}{2L} \sum_{j=1}^{L} \log_2 \left(1 + \frac{\sigma_{x_j}^2}{\sigma_{i_j}^2 + \sigma_{p_j}^2} \right) \quad (1)$$

In most watermarking applications, σ_x^2 is calculated according to perceptibility requirements. For instance in [9] $\sigma_{x_j}^2$ is replaced by the visual threshold of band j. In other words, $\sigma_{x_j}^2$ is the maximum message signal energy permitted in band j based on its perceptual quality effects. This parameter also depends on the magnitude of the particular coefficient. Due to the properties of human visual system, a coefficient with larger magnitude can be altered to a larger extent than a coefficient with smaller magnitude. Our goal is to have an estimate of the average energy that can be added to a particular band. Since the human visual system is more sensitive to lower frequency bands than higher ones, and lower frequency bands have higher variance, a reasonable model for the visual threshold can be [9]

$$\sigma_{x_j}^2 = k\sigma_{i_j}^{2\alpha} \quad (2)$$

where $0 \le \alpha \le 1$, and $k \langle\langle \sigma_{i_j}$, and σ_{i_j} is the variance of the coefficients in band j.

In some scenarios such as automatic biometric user authentication, where recognition is done automatically, human perception will be of less importance. In these cases, the energy of message signal can be distributed equally among different bands regardless of their variances. In this paper, we set $\alpha = 0$ and calculate the capacity for different values of k .

Channel noise is the sum of two noise sources, image noise with variance σ_i^2 and processing noise with variance σ_p^2. In order to model the image noise, we assume that $f_{I_j}(i_j)$ is the distribution of the jth subband of the host image. The image noise is split into its components in L subbands which are modeled as random variables with variance $\sigma^2_{i_j}$. The next step is to obtain their entropy equivalent Gaussian variances (or the Gaussian random variable that has the same entropy as these random variables). This is achieved by plotting a histogram of the coefficients of each band and calculating the entropy. If Δx is the width of n bins of the histogram $g_i(m), m = 1,2,...,n$ and p is the total number of coefficients in band j, the entropy and the equivalent Gaussian variance $\sigma^2_{i_j}$ are obtained as

$$H_j = -\sum_{i=1}^{n} \frac{g_j(i)}{p\Delta x} \log_2 (\frac{g(i)}{p\Delta x}) \Delta x \qquad (3)$$

$$\sigma^2_{i_j} = 2^{2H_j / 2\pi e}$$

Thus the image noise in subband j can be replaced by a Gaussian noise of variance $\sigma^2_{i_j}$ [9]. Note that this noise source can be omitted in non-blind approaches, since the image noise can be subtracted from the received image. Therefore, we expect such schemes to have higher capacity than blind watermarking approaches.

The processing noise is estimated as the variance of an equivalent additive noise which substitutes the actual (nonlinear) processing noise sources [9], such as JPEG compression and gamma correction. We define processing noise as the equivalent additive noise which accounts for the reduction in correlation between the transform coefficients of the original image and the transform coefficients of the image obtained after processing. We assume the processing noise in each subband as $\sigma^2_{p_j}, j = 1,...,L$. In order to obtain this variance, we apply the processing to n_i test images and decompose both the original and processed images into L subbands. Thus we will obtain MNn_i / L samples for each subband. Let $c_{j_k}, k = 1,...,(MNn_i)/L$ be the coefficients of band j of test images and $\tilde{c}_{j_k}, k = 1,...,(MNn_i)/L$ be the corresponding coefficients of the images subjected to processing. The variance of processing noise is obtained as follows:

$$\frac{\langle c_j, \tilde{c}_j \rangle}{|c_j||\tilde{c}_j|} = \frac{\langle c_j, (c_j + n_j) \rangle}{|c_j||c_j + n_j|} = \rho_j \qquad (4)$$

$$\sigma^2_{p_j} = (\frac{1}{\rho^2_j} - 1)|c_j|^2$$

In the next section, image noise and processing noise are estimated for fingerprint and iris images based on the above equations by means of simulations.

5- Experimental results

We estimate data hiding capacity for two databases of fingerprint images (364×328 pixels) and iris images (576×768 pixels). The images were decomposed into L=10 subbands by applying two dimensional wavelet transform. We used 4-tab Daubechies filters for wavelet decomposition of images. We have assumed that the watermarked image may be subjected to different types of attacks including median filtering, JPEG compression, Gaussian filtering, sharpening and addition of Gaussian noise. We estimated the noise due to these attacks and figured out that in order for the images to resist these attacks how many bits can be hidden in them. In other words, acceptable capacities for these images were estimated in order to be robust against different attacks. Since we have focused on data hiding for automatic user authentication schemes, we are able to eliminate the effect of human visual system on designing watermarking algorithms. Thus we choose $\alpha = 0$ in Equation (2) so that message energy is distributed equally among different subbands. The constant k is chosen to be smaller than the variance of the coefficients of each subbands.

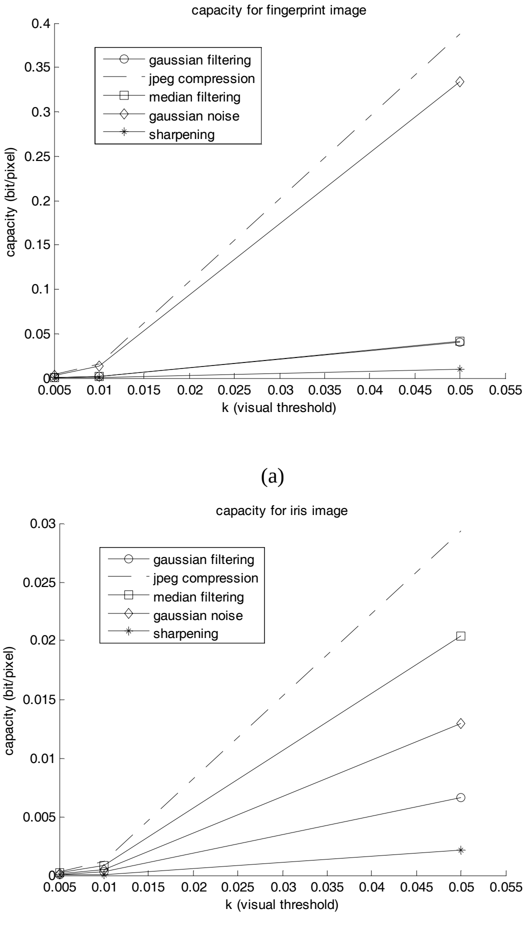
Also since we are targeting user authentication applications, we use non-blind data-hiding, as a result we have omitted the variance of image noise σ_i^2. The variance of processing noise σ_p^2 is estimated according to Equaion (4). So the capacity of data hiding channel is given by

$$C = \frac{MN}{2L}\sum_{j=1}^{L}\log_2(1+\frac{k}{\sigma_{p_j}^2}) \qquad (5)$$

The estimated capacity for different values of k in the presence of different kind of attacks is shown in Fig.4 and Fig.5 for the following two cases:

- Case A: We have assumed that all coefficients of each subband can be used for data hiding.
- Case B: We have assumed only the coefficients of QSWT are considered as data hiding channels.

It is shown that in the first case, fingerprint images provide more capacity for data hiding in comparison with iris images. In our simulations, constant k indicates the energy of the message to be hidden. It is shown that increasing k has no effect in increasing capacity in the presence of sharpening attacks. In other words, increasing message energy is not appropriate for achieving higher capacity in these cases. This is true because sharpening is a kind of high pass filtering and we assumed that the data is hidden in mid and high frequency bands. Also by using QSWT algorithm, the total capacity will increase. This is more obvious for iris images.



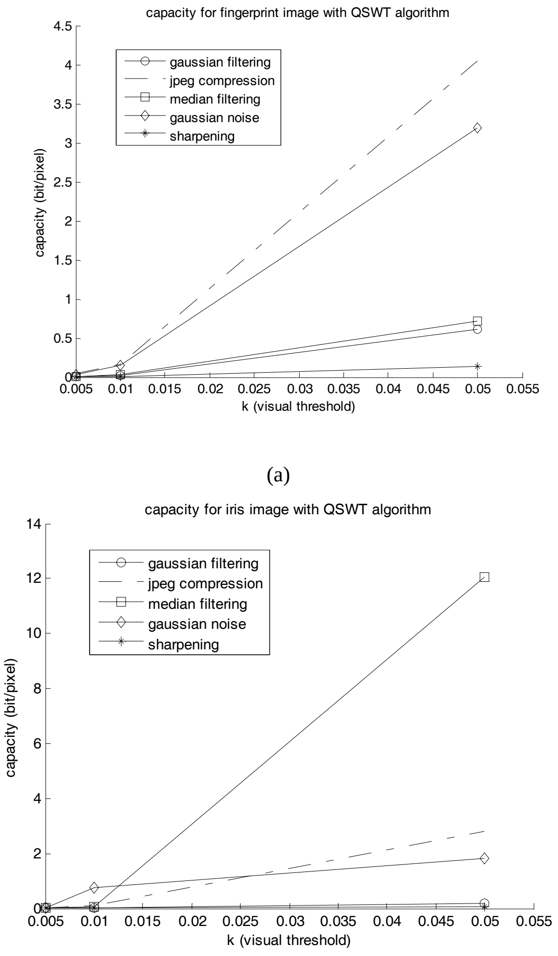
(a)

(b)

Fig 4. Capacity estimates (case A) a) fingerprint images, b) iris images

6- Conclusion

We have presented a technique for estimating the data hiding capacity of biometric images for user authentication applications. Since human perception is of less importance in such scenarios, the message energy can be distributed equally among different subbands of wavelet transform. Our experimental results show that increasing message energy will increase data hiding capacity, although other properties such as visual perception may decrease. Also it was shown that the QSWT algorithm will increase the capacity.



(a)

(b)

Fig. 5. Capacity estimates (case B) for a) fingerprint image b) iris image

Also increasing message energy in the presence of compression and Gaussian noise will cause a significant increase in the capacity but in the case of sharpening and filtering message energy does not have any significant effect on data hiding capacity.

7- References

[1] P. Moulin, M. K. Mihcak, "A framework for evaluating the data-hiding capacity of image sources", *IEEE Trans. Image Processing*, Vol. 11, No. 9, September 2002.

[2] S. D. Servetto, C. I. Podilchunk, K. Ramchandran, "Capacity issues in digital image watermarking", *IEEE Intl. Conf. on Image processing*, 1998, volume 1.

[3] P. Moulin, M. K. Mihcak, "A framework for evaluating the data hiding capacity of image sources", *IEEE Trans. Image processing*, vol. 11, no. 9, 2002.

[4] C. Y. Lin, S. F. Chang, "Zero-error information hiding capacity of digital images", *IEEE Intl. conf. on image processing*, vol.3 2001.

[5] Z. Fan, Z. Hongbin, "Wavelet domain watermarking capacity analysis", *proc. SPIE* Vol. 5637, 2005.

[6] N. K. Ratha, J. H. Connel, R. M. Bolle, "Enhancing security and privacy in biometric-based authentication systems", *IBM Systems Journal*, Vol. 40, No. 3, 2001.

[7] M. Hsieh, D. Tseng, Y. Huang, "Hiding digital watermarks using multiresolution wavelet transform", *IEEE Trans. On industrial electronics*, vol. 48, No. 5, Oct 2001.

[8] B. McKinnon, X. Qi, "Adaptive wavelet-based family tree quantization for digital image watermarking",

[9] M. Ramkumar, A. N. Akansu, "Capacity estimates for data hiding in compressed images", *IEEE Trans. Image Processing*, Vol. 10, No. 8, August 2001.

[10] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, 2^{nd}, Ed. New York, Wiley, 1991.