Multiple Description Coding for Image Data Hiding Jointly in the Spatial and DCT Domains

Mohsen Ashourian[1] and Yo-Sung Ho[2]

[1] Azad University of Iran, Majlesi Branch
P.O. Box 86315-111, Isfahan, Iran
mohsena@iaumajlesi.ac.ir

[2] Kwangju Institute of Science and Technology (K-JIST)
1 Oryong-dong Puk-gu, Kwangju, 500-712, Korea
hoyo@kjist.ac.kr

Abstract. In this paper, we propose a new method for hiding a signature image in the host image. We encode the signature image by a balanced two-description subband coder and embed the descriptions in the different portions of the host image. We split the host image into two images from its even and odd rows, and embed the information of one signature description in the first portion of the host image in the spatial domain, and the other description in the second portion in the DCT domain. In both cases, we employ proper masking operation to reduce visibility of embedded information in the host image. At the receiver, the multiple description decoder combines the information of each description to reconstruct the original signature image. We experiment the proposed scheme for embedding gray-scale signature images of 128×128 pixels in the gray-scale host image of 512×512 pixels, and evaluate the system robustness to various attacks.

1 Introduction

In data hiding schemes, perceptually invisible changes are made to image pixels for embedding additional information [1]. Data hiding can be used to embed control or reference information in digital multimedia data for various applications, such as tracking the use of a particular video for pay-per-view, billing for commercials in audio/video broadcast, and for watermarking. Unlike traditional encryption methods where it is obvious that some information is encoded, perceptually invisible data hiding in image or video offers an alternative approach for secret information transmission.

Main features of the image data hiding scheme are the method of encoding a signature image and the way to embed the signature information into the host information. In the image hiding method given by Chae and Manjunath [2], the signature image is encoded using lattice vector quantization of its subbands. An improved version of the above system using channel optimized vector quantization for the signature signal encoding is also suggested [3]. Both methods are robust to JPEG compression

S. Qing, D. Gollmann, and J. Zhou (Eds.): ICICS 2003, LNCS 2836, pp. 179–190, 2003.

and addition of noise; however, they are not robust to some attacks, such as cropping and down-sampling.

In this paper, we suggest to use a multiple description coding method for encoding the signature image and embedding the information of the two descriptions in both the spatial and DCT domains of the host image. The main advantage of encoding the signature image by two descriptions and embedding these descriptors in the host signal is that with an appropriate strategy, we can reconstruct a high quality signature signal when we receive both descriptions without any error. On the other hand, if the host signal is attacked, we can retrieve a less corrupted description from the host image and reconstruct an acceptable quality signature image using the less corrupted description.

After we provide an overview of the proposed image hiding system in Section 2, we explain the encoding process of the signature image using multiple description coding in Section 3. Section 4 and Section 5 explain the data embedding and extraction processes respectively. Finally we present experimental results of the proposed scheme in Section 6, and summarize the paper in Section 7.

2 Overview of the Proposed Method

Fig. 1 shows the overall structure of the proposed system for signature image embedding. We encode the signature image using a two-description subband coder. The output of two descriptions are represented by D_o and D_e. The host image is divided into two parts of its odd and even rows, I_o and I_e, which are analogues to the two communication channels. The bit stream of the first description D_o, is embedded in the spatial domain of I_o, and the bit stream of the other description D_e, is embedded in the DCT domain of I_e.

Fig. 2 shows the block diagram of recovering the signature image at the receiver. We use the original host image and the received host image to recover the two descriptions, and reconstruct the signature image using the MDC subband decoder.

3 Multiple Description Coding of the Signature Image

Multiple description coding (MDC) was originally proposed for speech transmission over noisy channels [4]. El-Gamal and Cover provided the information-theoretic analysis of MDC [5], and Vaishampayan devised a method for the multiple description scalar quantizer design [6]. Recently, MDC has been studied as an approach for transmission of compressed visual information over error prone environments [7]. Various MDC schemes for images have been proposed for wireless and computer network applications [7]. In this paper, we develop a fixed rate MDC subband image coder using multiple description scalar quantization for the subband signals.

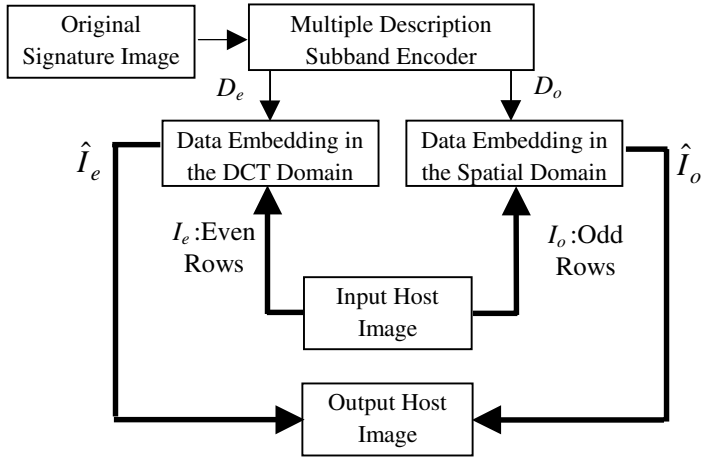

Fig. 1. Signature image embedding in the host image

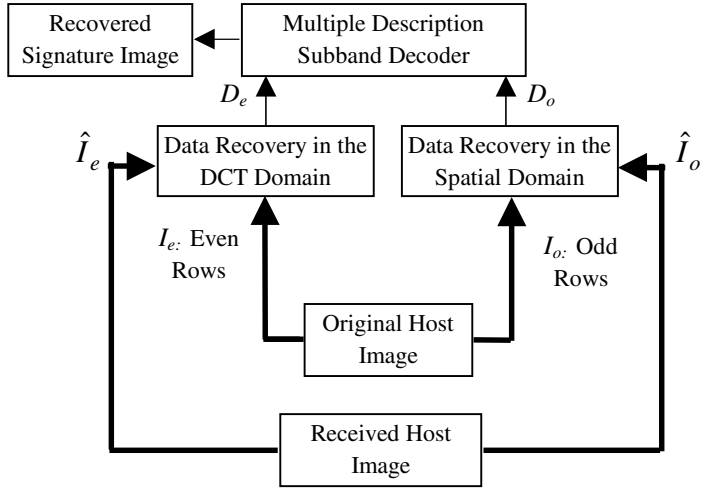

Fig. 2. Signature image recovery

In the first stage for signature image encoding, we decompose the signature image using the Haar wavelet transform, resulting in four subbands usually referred to as LL, LH, HL and HH. Except for the lowest frequency subband (LL), the probability density function (PDF) for other subbands can be closely approximated with the Laplacian distribution. Although the LL subband does not follow any fixed PDF, it contains the most important visual information. We use a phase scrambling operation to change the PDF of this band to a nearly Gaussian shape [8]. Fig. 3 gives the block schematic of the phase scrambling method. As shown in Fig. 3, the fast Fourier transform (FFT) operation is performed on the subband and then a pseudo-random noise is added to the

phase of its transformed coefficients. The added random phase could be an additional secret key between the transmitter and the registered receiver.

We encode the subbands using a PDF-optimized two-description scalar quantizer, assuming the Laplacian distribution for high frequency bands, and the Gaussian distribution for the LL subband after phase scrambling. We devise index assignments scheme for subband scalar quantizers with different output bit-rates [6]. A sample of index assignment for the three bits quantizer is shown in Fig. 4, where rows and columns are quantization indices of the first and second descriptions.

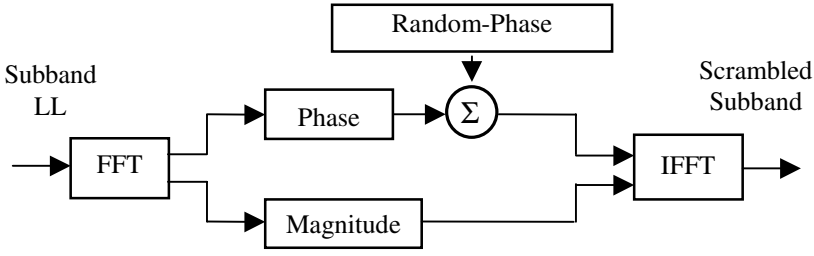

Fig. 3. Phase-Scrambling of lowest frequency subband

	1	2	3	4	5	6	7	8
1	●	●	●					
2	●	●	●	●				
3	●	●	●	●	●			
4		●	●	●	●	●		
5			●	●	●	●	●	
6				●	●	●	●	●
7					●	●	●	●
8						●	●	●

Fig. 4. Sample of index assignment used for subband multiple description scalar quantizers

In this paper, we have set the image encoding bit-rate at three bit per sample (bps), and obtained PSNR value over 31 dB for different tested images, which is satisfactory in image hiding applications [1]. We use an integer bit-allocation scheme among the four subbands based on their energies. The information of subband energies (15 bits) can be sent as side information or can be encoded with a highly robust error correction method and embedded in the host image.

We use the folded binary code (FBC) for representing output indices of quantizer to have higher error resilience and scramble the output indices of each description and arrange the indices as two binary sequences $D_e = d_{e,1}, d_{e,2}, ..., d_{e,n}$ and $D_o = d_{o,1}, d_{o,2}, ..., d_{o,n}$. In order to embed the data, we change the binary elements of the sequences to bipolar bits by mapping each bit form {0,1} to {-1,1}.

4 Data Embedding in the Host Image

The data embedding in the host image could be in the spatial or frequency domain [1]. While data embedding in the spatial domain is more robust to geometrical attacks, such as cropping and down-sampling, data embedding in the frequency domain usually has more robustness to signal processing attacks, such as addition of noise, compression and lowpass filtering [1].

As shown in Fig.1, we use data embedding in both spatial and DCT domains. We make two images, I_e and I_o, from even and odd rows of the host image. One description of the signature image is embedded in the spatial domain of I_e, and the other description is embedded in the DCT domain of I_o. In fact, transmission channels for the two signature image descriptions are I_e and I_o. In the proposed system, we need the host image at the receiver for signature image recovery; however, using different methods for embedding information in the texture area of the host image [1], this system can be easily extended for blind image hiding applications.

4.1 Data Embedding in the Spatial Domain

We embed each element of the binary sequence $D_o = d_{o,1}, d_{o,2}, ..., d_{o,n}$ in a pixel $x_{i,j} \in I_o$ by

$$\hat{x}_{i,j} = x_{i,j} + M(i,j) \cdot \alpha_o \cdot d_{o,k} \tag{1}$$

where the positive scaling factor α_o determines the modulation amplitude of the watermark signal in the spatial domain, and $M(i,j)$ is a spatial masking vector derived from the normalized absolute value of the gradient vector $G(i,j)$ at $x_{i,j}$.

$$M(i,j) = 0.5 * (1 + |G(i,j)|) \tag{2}$$

4.2 Data Embedding in the DCT Domain

We embed the second descriptor of the signature image in the second portion of the host image I_e. We distribute the bit stream $D_e = d_{e,1}, d_{e,2}, ..., d_{e,n}$ among the 8×8 pixel blocks. The new DCT coefficients of the k^{th} block ($\hat{W}^k_{i,j}$) can be obtained from the original coefficients ($W^k_{i,j}$) by

$$\hat{W}^k_{i,j} = W^k_{i,j} + N_k(i,j) \cdot \alpha_e \cdot d_{e,m} \tag{3}$$

where N_k is a masking matrix derived from the DCT coefficients of each block using the Watson model [9], and the positive scaling factor α_e determines the modulation

amplitude of embedded signal in the DCT domain. In practice, since the size of signature image is smaller than the host image size, we only embed data in DCT coefficients of middle frequency bands.

5 Signature Image Recovery

Fig. 2 shows the process of signature image recovery. We use the original host image and the received host image to derive the even portion ($I_e, \hat{I}_e$), and the odd portion ($I_o, \hat{I}_o$). For recovering the description embedded in the spatial domain using the original image pixels $x_{i,j} \in I_o$ and the received image pixel $\hat{x}_{i,j} \in \hat{I}_o$, we extract the embedded bits by

$$\hat{d}_{e,k} = 0.5 * (sign(\frac{\hat{x}_{i,j} - x_{i,j}}{\alpha_o \cdot M(i,j)}) + 1) \tag{4}$$

and since $M(i,j)$ and α_o are positive parameters, Eq. 4 can be simplified to

$$\hat{d}_{e,k} = 0.5 * (sign(\hat{x}_{i,j} - x_{i,j}) + 1) . \tag{5}$$

Similarly, we derive the description embedded in the DCT domain by subtracting the DCT coefficients of the received image from the original DCT coefficients of I_e.

$$\hat{d}_{o,k} = 0.5 * (sign(\frac{\hat{W}^k_{i,j} - W^k_{i,j}}{\alpha_e \cdot N_k(i,j)}) + 1) \tag{6}$$

and since $N_k(i,j)$ and α_e are positive parameters, Eq. 6 can be simplified to

$$\hat{d}_{o,k} = 0.5 * (sign(\hat{W}^k_{i,j} - W^k_{i,j}) + 1) . \tag{7}$$

The subband quantization indices are obtained by proper arrangement of the extracted bits. Considering the multiple description scheme that has been used in information embedding, we can reconstruct three signature images based on each descriptor alone or based on their combinations. The receiver uses the index assignment, as illustrated for the three bit quantizer in Fig. 4, and reconstructs each subband. When the reconstructed indices of the two descriptions are very far, we assume that one of the two descriptions has been corrupted highly by noise; therefore, by comparing the MSE value of the original host image and the reconstructed one in the area contains those descriptions, we can decide which index should be selected.

6 Experimental Results and Analysis

In our scheme, the host image should be at least 6 times larger in size than the signature image, because we use two descriptions with three bits per pixel quantization. We use a gray-scale host image of 512×512 pixels and signature image of 128×128 pixels. We use "Lena" image as the host image for all the experiments. In order to control the host image distortion by data embedding, we can change the embedding factor in the spatial and DCT domains. We set the two modulation factors, α_e and α_o, such that the host image PSNR stays above 35 dB for our experiments. Fig. 5 shows the host image after data embedding.

Fig. 5. The host image after data embedding

We arrange two series of experiments. For image hiding application, two images, "Barbara" and "Elaine", are used as signature images, and for watermarking application, the "IEEE" logo image is used. Fig. 6 shows reconstructed signature images and Fig. 7 shows the reconstructed logo image.

For data hiding for image transmission applications, PSNR values of reconstructed signature images are given. For copyright protection, we should make a binary decision for the presence or absence of the signature image because the presence of the signature is important rather than the quality of reconstructed image. We define the similarity factor between the recovered logo image $\hat{s}(m,n)$ and the original signal $s(m,n)$ as

$$\rho = \frac{\sum_{m,n} \hat{s}(m,n)s(m,n)}{\sum_{m,n} (\hat{s}(m,n))^2} \tag{8}$$

Based on the value of ρ, we make a decision on the presence ($\rho = 1$), or absence of the logo image ($\rho = 0$). We provide PSNR value and ρ for several main types of attacks for evaluating system performance.

Robustness to Gaussian Noise: We add Gaussian noise with a different variance to the normalized host signal after signature embedding. Fig. 8 shows the PSNR values of signature images for additive noise with different variances. From Fig. 8, we conclude from this figure that for certain range of noise, our strategy shows good performance in resisting Gaussian noise for data hiding applications.

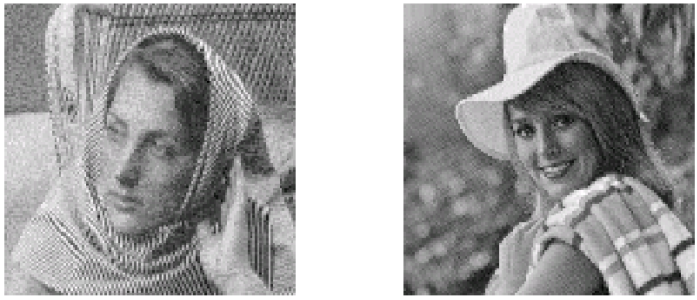

Fig. 6. Reconstructed signature images

Fig. 7. Reconstructed logo image

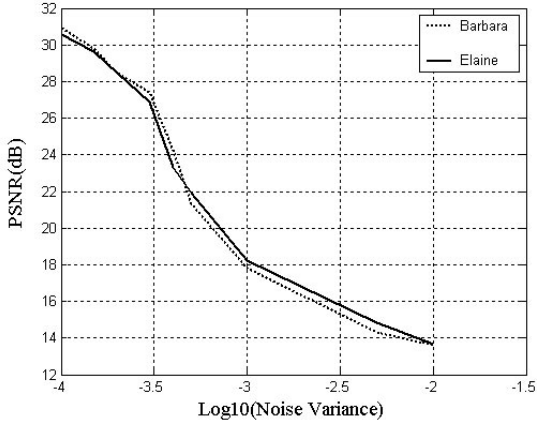

Fig. 8. PSNR variation of recovered signature images for additive Gaussian noises

Fig. 9 shows the value of similarity factor (ρ) for the hidden logo. We can see that even at high additive noise, the ρ value is higher than 0.75, which means the possibility of watermark recovery.

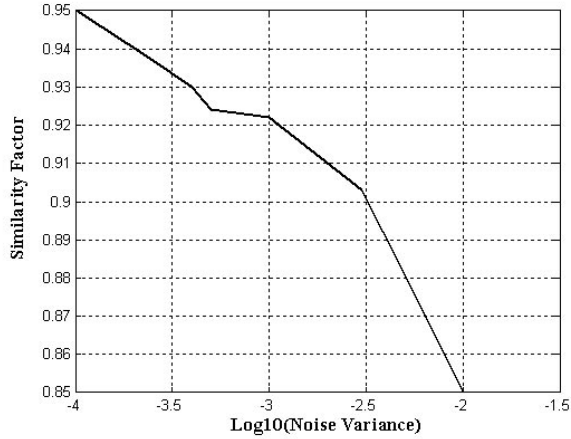

Fig. 9. Similarity factor variation of logo image for additive Gaussian noises

Resistance to JPEG Compression: The JPEG lossy compression algorithm with different quality factors (Q) is tested. Fig. 10 shows the PSNR variation for different Q factors and Fig. 11 shows the similarity factor variation due to JPEG compression for the logo image. As shown in these figures, PSNR values drop sharply for Q smaller than 50 , and ρ drops for Q smaller than 40.

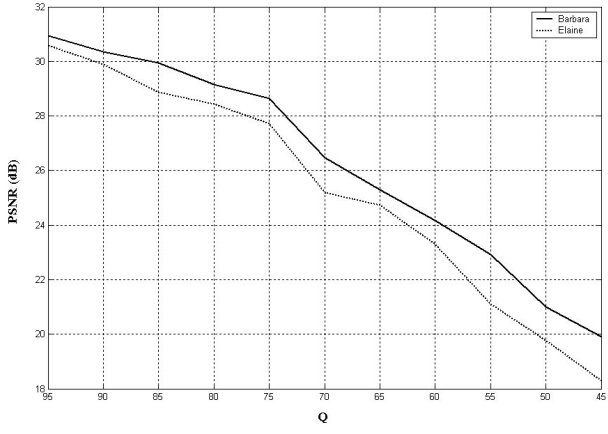

Fig. 10. PSNR variation of recovered signature images due to JPEG compression

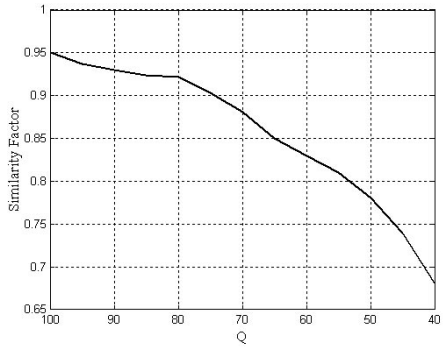

Fig. 11. Similarity factor variation of recovered logo image due to JPEG compression

Resistance to Median and Gaussian Filtering: Median and Gaussian filters of 3×3 mask size are implemented on the host image after embedding the signature. We choose the Gaussian filter standard deviation equal to 0.5. PSNR values of recovered signature image are listed in Table 1, and the similarity factors for the recovered logo image are listed in Table 2.

Table 1. PSNR (dB) values of the recovered signature images after implementing median and Gaussian filters on the host image

	Median Filter	Gaussian Filter
Barbara	21.90	26.80
Elaine	20.65	25.82

Table 2. Similarity factor values of the recovered logo images after implementing median and Gaussian filters on the host image

	Median Filter	Gaussian Filter
ρ	0.80	0.85

Resistance to Cropping: In our experiment, we have cropped parts of the host image coroners. Fig. 12 shows a sample of the host image after 20% cropping. We fill the cropped area with the average value of the remaining part of the image. Table 3 shows PSNR values and Table 4 shows the similarity factor when some parts of the host image corners are cropped. Considerably good resistance is due to the existence of two descriptors in the image and scrambling of embedded information, which makes it possible to reconstruct the signature image information partly in the cropped area from the available descriptor in the non-cropped area.

Fig. 12. Sample of the host image with embedded data after 20% cropping

Table 3. PSNR (dB) values of the recovered signature image for different percentage of cropping the host image

	5%	10%	15%	20%
Barbara	24.58	22.42	21.60	20.92
Elaine	24.15	23.04	22.10	20.01

Table 4. Similarity Factor values of the recovered logo image for different percentage of cropping the host image

	5%	10%	15%	20%
ρ	0.92	0.84	0.760	0.69

Resistance to Down-sampling: Table 5 shows results of PSNR values of recovered signature image, and Table 6 shows results of similarity factor for the logo image after several down-sampling processes. Due to loss of information in the down-sampling process, the host image cannot be recovered perfectly after up-sampling. However, it is possible to recover the signature image from the available host image pixels in the spatial domain.

Table 5. PSNR (dB) values of the recovered signature image after different amount of down-sampling the host image

	1/2	1/4	1/8
Barbara	27.18	21.1	18.2
Elaine	28.03	21.3	16.7

Table 6. Similarity factor of the recovered logo image after different amount of down-sampling the host image

	1/2	1/4	1/8
ρ	0.82	0.76	0.67

7 Conclusion

We have presented a new image hiding scheme for embedding a gray-scale image into another gray-scale image based on multiple description subband image coding, and data embedding jointly in the spatial and DCT domains. We examined the system performance for signature image embedding in another image for secure transmission, and for logo image embedding for watermarking purpose. As results show, multiple description coding of signature image and embedding in different domains make it possible to recover the signature signal with good quality even when the host image undergoes different geometrical and signal processing operations. The system performance could be further improved by estimating the image data hiding capacity in the different domains [10] and using it for optimum bit allocation among the descriptors.

Acknowledgements. This work was supported in part by Kwangju Institute of Science and Technology (K-JIST), in part by the Korea Science and Engineering Foundation (KOSEF) through the Ultra-Fast Fiber-Optic Networks (UFON) Research Center at K-JIST, and in part by the Ministry of Education (MOE) through the Brain Korea 21 (BK21) project.

References

1. Petitcolas, F.A.P., Anderson, R.J., and Kuhn, M.G.: Information Hiding-a Survey. Proceedings of the IEEE, Vol. 87, No.7, (1999)1062–1078.
2. Chae, J.J., and Manjunath, B.S.: A Robust Embedded Data from Wavelet Coefficients. Proceeding of SPIE, Storage and Retrieval for Image and Video Databases VI, (1998) 308–317.
3. Mukherjee, D., Chae, J.J., Mitra, S.K., and Manjunath, B.S.: A Source and Channel-Coding Framework for Vector-Based Data Hiding in Video. IEEE Transaction on Circuits and System for Video Technology. Vol. 10, No. 6, (2000)630-645.
4. Jayant, N.S.: Sub-sampling of a DPCM Speech Channel to Provide Two Self-contained Half-rate Channels. Bell System Technical Journal, Vol. 60, No. 4, (1981)501–509.
5. El-Gamal, A.A., and Cover, T.M.: Achievable Rates for Multiple Descriptions. IEEE Trans. on Information Theory, Vol. 28, No. 11, (1982) 851–857.
6. Vaishampayan, V.A.: Design of Multiple Description Scalar Quantizers. IEEE Trans. on Information Theory, Vol. 39 , No.5, (1993) 821–834.
7. Goyal, V.K.: Multiple Description Coding: Compression Meets the Network. IEEE Signal Processing Magazine, Vo.18, Issue 5, (2001)74–93.
8. Kuo, C.C.J., and Hung, C.H.: Robust Coding Technique-Transform Encryption Coding for Noisy Communications. Optical Engineering, Vol. 32, No. 1, (1993)150–153.
9. Wolfgang, R.B., Podilchuk, C.I., and Delp, E.J.: Perceptual watermarks for digital images and video. Proceedings of the IEEE, Vol. 87, No. 7, (1999)1108–1126.
10. Moulin, P., and O'Sullivan, J.A.: Information-theoretic analysis of information hiding. IEEE Transactions on Information Theory, Vol.49, No.3, (2003)563–593.