ESTIMATING AND UNDOING ROTATION FOR PRINT-SCAN RESILIENT DATA HIDING

K. Solanki, U. Madhow, B. S. Manjunath, and S. Chandrasekaran

Dept. of Electrical and Computer Engineering
University of California at Santa Barbara
Santa Barbara, CA 93106

ABSTRACT

This paper proposes a method to hide information into images that achieves robustness against printing and scanning with blind decoding. A significant contribution of this paper is a technique to estimate and undo rotation. The method is based on the fact that laser printers use an ordered digital halftoning algorithm for printing. Using the proposed hiding method, several hundred information bits can be embedded into 512×512 images with perfect recovery against the print-scan operation. Moreover, the hidden images also survive other attacks such as Gaussian or median filtering, scaling or aspect ratio change, heavy JPEG compression, and rows and/or columns removal.

1. INTRODUCTION

The advent of digital age with the internet revolution has made it extremely convenient for users to create, manipulate, and exchange multimedia information. This has created an urgent need for protecting intellectual property in both the digital and the print media. The ease with which images can be converted from print to digital form and vice versa, makes it necessary that copyright information be embedded into the images in such a way that the hidden information remains with the images even when they are printed and/or scanned.

Strong deterrents against forgery of important documents, such as passports, driving licenses, and ID cards are necessary at this time, when the concerns over security are higher than ever before. A viable solution is offered by print-scan resilient data hiding, wherein, information can be embedded into pictures in the documents, which can be decoded using specific devices that have access to a secret key. Forgery of such documents become extremely difficult because the embedded data is inseparable from the printed picture.

In this paper, we present a method for hiding information in images in a manner that is robust to printing and scanning. Original image is not required at the decoder. The method is based on embedding in the transform domain, with synchronization and error correction using powerful turbo-like channel codes. The design is based on an experimental understanding of the effects of the print-scan operation. An earlier version of this technique, along with preliminary results, was presented in [1]. An important new contribution of the present paper is a method for estimating the rotation undergone by the image during the scanning process, by exploiting knowledge of the digital halftoning scheme employed by the printer.

This research is supported in part by a grant from ONR # N00014-01-1-0380. Corresponding author email: solanki@ece.ucsb.edu

There has been a growing interest among researchers in the area of print-scan resilient data hiding. Many watermarking methods have been proposed, that embed a watermark into an image, which can be detected after it is printed and scanned (for example, [2],[3],[4],[5]). Ruanaidh and Pun [2] propose a watermarking method based on log polar map of discrete Fourier transform (DFT) magnitudes (i.e., the Fourier-Mellin or FM transform). Lin et al [3] propose a model for the print-scan process by considering pixel value and geometric distortions separately. They also use FM transform to hide information. Technique proposed in [4] involves DFT magnitudes as well, but the watermark itself is made circularly symmetric so that the log polar coordinate transformation is not required. Bas et al [5] use geometrically invariant feature points to embed the watermark. A few approaches focus on hiding in halftone images (e.g., [6],[7]). In these methods, the halftone cells of the host image are shifted in different ways based on the data to be hidden and composite halftone images are given out directly.

Our method, named 'selective embedding in low frequencies' (SELF) is also based on DFT magnitudes, but is quite different from the above schemes. Experimental channel modeling of the print-scan process has been done leading to a number of new findings regarding the channel behavior. This forms the basis of the proposed embedding scheme, in which information is hidden only in dynamically selected low frequency DFT coefficients. In previous work (e.g., [3, 4]), a predefined set of mid frequency coefficients were used for embedding. We also employ turbo-like error and erasure correcting codes in a novel fashion to counter the synchronization problem caused due to image-adaptive hiding. This also provides robustness to the hidden data against a variety of other attacks such as those in *Stirmark* [8], e.g., heavy JPEG compression, scaling or aspect ratio change, Gaussian or median filtering, rows and/or columns removal, and random bending.

Prior to decoding, the scanned digital image is preprocessed by an automated algorithm for estimating and undoing the rotation caused by random placement of the printed image in the scanner. The method is based on the fact that laser printers use an ordered digital halftoning algorithm for printing. The employed derotation method is completely different from the previously used approaches, in which rotation invariance is typically achieved by using FM transform [2, 3]. The advantage of the proposed technique for print-scan resilient hiding is that there is no penalty in hiding rate for achieving robustness against rotation. In fact, as stated in Section 4, the estimation and automatic derotation allows more information to be hidden (as compared to manual placing of image printout on the scanner flatbed) because of its accurate estimation of the rotation angle. It should be noted that the proposed derotation technique cannot be applied to a general rotation attack (e.g., if the image is rotated digitally) since it uses the printer halftone screen to estimate the rotation angle.

We are able to hide several hundred bits into 512×512 images against the print-scan attack with blind decoding (i.e., not assuming availability of original image at the decoder). Moreover, unlike [3] and [4], the receiver does not assume the availability of the hidden data (or the watermark sequence); rather it decodes the hidden information bits. Our method does not assume control over the halftone cells (as in [6],[7]), and do not output halftone images directly.

2. PRINT-SCAN RESILIENT HIDING

In this section we first present our results on the print-scan channel characterization followed by a hiding method based on the channel model. Next, we describe a coding framework used to counter synchronization problem caused due to image-adaptive hiding.

2.1. The Print-Scan Channel

We printed and scanned several grayscale images using commercially available printer and scanner. Specifically, Lexmark Optra S 1620 laser printer and CanoScan N670U flatbed scanner were used. In the experiments, we assume a degree of control over the printing and the scanning operation. The images were printed at high resolution, with several dots dedicated to one pixel, e.g., a 512×512 image is printed (at 300 or 600 dpi printer resolution) on an A4 page with 72 pixels per inch, such that the size of the image on the paper is 7.11"×7.11". The images were printed and scanned at varying resolutions (300 to 1200 dpi for printing, and 75 to 1200 dpi for scanning). Commonly used Xerox recycled papers (for copiers and laser/inkjet printers) were used for printing. Note that explicit registration of the scanned and original image features is not performed since it is assumed that the original image is not available at the decoder.

Various parameters, such as printer and scanner resolutions, scanner gamma correction, and print image size were varied and its effect on the image features were studied in order to find features that are invariant to the print-scan operation. Some interesting trends in the DFT coefficient magnitudes were discovered, as listed below.

1. The low and mid frequency coefficients are preserved much better than the high frequency ones. In general, the lower the frequency, the better its chances of surviving the print-scan process.
2. In the low and mid frequency bands, the coefficients with low magnitudes see a much higher noise than their neighbors with high magnitudes.
3. Coefficients with higher magnitudes (which do not get severely corrupted) see a gain of roughly unity (with the default gamma correction applied at the scanner). Roughly speaking, if the print-scan operation is approximated as a linear filter (for large enough coefficients and low enough frequencies), then the magnitude gain is unity after application of gamma correction. One possible explanation is that the printing operation in itself does not cause blurring, since several dots are dedicated to each pixel of a printed image.
4. Slight modifications to the selected high magnitude low frequency coefficients does not cause significant perceptual distortion to the image.

2.2. Selective Embedding in Low Frequencies

Based on the experimental modeling described in the previous section, we propose a new image-adaptive hiding method that achieves robustness against the print-scan operation. Information is hidden only in dynamically selected low frequency coefficients whose magnitude is greater than a predefined threshold. Hence the name: selective embedding in low frequencies (SELF).

Consider an N×N host image in which data is to be hidden. Let us denote the natural logarithm of the magnitudes of 2D DFT of the whole image by c_{ij}, $0 \leq i, j \leq N-1$. We embed in a given coefficient c_{ij} only if it lies in a predetermined frequency band and also exceeds a threshold t_{ij}. Let us define the band as an indicator function b_{ij}, such that if $b_{ij} = 1$, the coefficient c_{ij} lies in the band. Note that b_{ij}, t_{ij} and the quantization interval Δ are design parameters that are shared between the encoder and the decoder. Data is embedded using choice of scalar quantizers. We either send $Q_1(c_{ij})$ or $Q_0(c_{ij})$ depending on the bit to be hidden. Thus, the modified coefficient, d_{ij} can be given as

$$d_{ij} = \begin{cases} Q_{b_l}(c_{ij}) \text{if } b_{ij} = 1, \text{ and } c_{ij} > t_{ij}, \\ c_{ij} \quad \text{otherwise.} \end{cases} \tag{1}$$

Note that during the embedding process, two symmetric coefficients are changed in the same manner so that the inverse DFT of the modified coefficients is always real.

2.3. Coding Framework for Synchronization

The method proposed above is an image-adaptive technique, in which, the encoder dynamically selects the coefficients to embed. The decoder does not have explicit knowledge of the locations where data is hidden, but employs the same criteria as the encoder to guess these locations. The distortion due to attacks may now lead to insertion errors (the decoder guessing that a coefficient has embedded data, when it actually does not) and deletion errors (the decoder guessing that a coefficient does not have embedded data, when it actually does). In principle, this can lead to desynchronization of the encoder and decoder.

An elegant solution based on erasures and errors correcting codes is provided to deal with the synchronization problem caused by the use of local adaptive criteria. This framework was first employed in our previous work on high volume data hiding ([9], [10]), in which a local adaptive criteria was used to preserve the perceptual quality of the hidden image.

The bit stream to be hidden is coded, using a low rate code, assuming that all host coefficients that lie in the candidate embedding band will actually be employed for hiding. A code symbol is *erased at the encoder* if the local adaptive criterion (i.e., the threshold criterion) for the coefficient is not met. We used repeat-accumulate (RA) codes [11] in our experiments because of their simplicity and near-capacity performance for erasure channels. A rate 1/q RA encoder involves q-fold repetition, pseudorandom interleaving, and accumulation of the resultant bit-stream. Decoding is performed iteratively using the sum-product algorithm [12].

Let us consider an example wherein we want to hide in a 512×512 image. The candidate embedding band is a design parameter known to both encoder and decoder. Let us assume that the band spans 1000 coefficients. Suppose we want to hide 200 bits into the image. We would use a 1/5 RA code (i.e., q = 5), which gives a codeword length of 1000. This codeword is now hidden using the adaptive criteria such that if a coefficient does not pass the threshold test, the corresponding code symbol is erased (i.e. not hidden). Note that the RA code rate and the number of bits hidden are predetermined at the design state, and are chosen in such a way that the codeword length is equal to, or slightly greater than the number of candidate embedding coefficients. When the codeword length is greater than the size of the band, the excess code symbols are erased at the encoder.

3. ESTIMATING AND UNDOING ROTATION

In this section, we present a method to estimate the angle of rotation an image might undergo during the print-scan process.

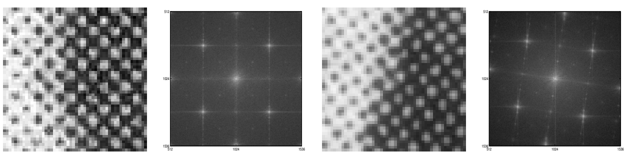
3.1. The Printing Process: Digital Halftoning

When an image is printed, it undergoes a continuous-tone to bilevel conversion, known as *digital halftoning*. Digital halftoning is required because almost all printers are bilevel devices. Several algorithms have evolved for digital halftoning over last decades. Readers are referred to [13] for an extensive discussion on halftoning methods.

We limit our attention to laser printers in this paper, which employ an ordered halftoning algorithm to generate the binary image. In ordered halftoning, the cells lie in a deterministic periodic array, which are oriented at an angle of 45 degrees for grayscale images. This is because there is a sharp minimum in perceptual sensitivity for spatial frequencies oriented at 45 degrees from horizontal. The halftone pattern can be captured by high resolution scanning and can be used to estimate and undo rotation as described in the following section.

3.2. Rotation Estimation

The angle by which an image gets rotated during the scanning process can be estimated using the fact that the halftone cells in the printout (of the image) are oriented at a 45 degree angle with the horizontal. Figure 1 (a) and (c) show magnified portions of a printed and scanned image without rotation and with rotation during scanning. Figure 1 (b) and (d) show the magnitude spectrum of the images in Figure 1 (a) and (c) respectively. Due to the orientation of the halftone cells, a peak can be seen at an angle of 45 degrees for the image without rotation. When the image gets rotated during the scanning process, the peaks also get rotated as in 1 (d). Note that a number of secondary peaks are observed, but only a part with the *primary* peaks is displayed here. The angle of the peak can be used to estimate the rotation and the image can be derotated before the hidden data is decoded.



(a) No rotation (b) Spectrum of (a) (c) With rotation (d) Spectrum of (c)

Fig. 1. Zoomed printed-and-scanned images and their Fourier spectra.

It should be noted that the Fourier transform is symmetric such that out of the four quadrants, the values are same for a pair of quadrants (for the displayed fft-shifted spectrum, quadrants I and III have same values and so do quadrants II and IV). The rotation angle can be estimated by measuring the angle of the peak in any of the four quadrants in the magnitude spectrum.

It is observed that the size of image on the printout is not exactly same as that in the digital form. For example, when a 512×512 image is printed with 72 pixels per inch, the height measured on the printout turns out to be about 0.05 inches longer than its width. Due to this discrepancy, the angle measured for a peak in the first quadrant of the Fourier magnitude spectrum is slightly different from that in the second quadrant. In practice, we use average of the two angles as an estimate of the rotation angle.

In the following we describe the algorithm used in estimating and derotating an image after scanning (at 600 dpi resolution).
(1) Crop a block of 2048×2048 pixels from the center of the scanned image and take its DFT.
(2) Find peaks (location of the maximum values) in the magnitude spectrum for the first and second quadrants. Let these angles (in degrees) be denoted by θ_1 and θ_2.
(3) Compute the estimate of the rotation angle as $\theta_r = (\theta_1 + \theta_2)/2 - 45$ and use bicubic interpolation to rotate the image by θ_r.
(4) The image is then cropped from the background by finding the edges with largest magnitudes of transition (first order difference) in intensity values.

Figure 2 shows the images at some of these intermediate stages. Figure 2 (a) and (b) show the original image and the composite image with 500 bits embedded. Figure 2 (c) shows the printed-and-scanned image which has been rotated during the scanning process. Figure 2 (d) shows the automatically derotated image (step (3)). Figure 2 (e) shows the image after the background is automatically cropped (step (4)).

Table 1. Number of information bits hidden along with RA code parameters used for various 512×512 images for the print-scan attack. The images with listed number of hidden bits also survive attacks such as 3×3 Gaussian filtering, 4×4 median filtering, heavy JPEG compression (QF = 10), 17 row and 5 columns removal, and aspect ratio change (by 0.8×1.00).

Image	# of bits hidden	RA code rate (1/q)	# of coeff. in band
Peppers	250	1/4	870
Baboon	475	1/6	2450
Bridge	250	1/7	1560
Man	500	1/5	2450
Couple	300	1/6	1560

4. RESULTS

Table 1 shows the number of information bits hidden for various 512×512 images along with the RA code rate and number of candidate embedding coefficients. The listed number of bits were recovered perfectly after the images were printed and scanned with varying degrees of rotation.

Table 2 compares the number of information bits hidden in various 512×512 images with automatic derotation at the decoder and with careful manual placing of the image on the flatbed of the scanner to avoid rotation. It can be seen that more information bits can be hidden when automatic derotation is performed at the

(a) Original 512×512 Man image

(b) Image with 500 bits hidden

(c) Printed and scanned image

(d) Automatically derotated image

(e) The derotated image cropped automatically

Fig. 2. Images at various stages of embedding, attack, and decoding.

Table 2. Comparison of number of information bits hidden in various 512×512 images in two scenarios: (i) automatic derotation at the decoder, and (ii) careful manual placing of the image printout on the scanner flatbed.

Image	Number of bits hidden	
	Auto. derotation	Manual placing
Peppers	250	225
Baboon	475	350
Bridge	250	200
Man	500	400
Couple	300	275

decoder as compared to careful manual placing without automatic derotation. It shows that automatic derotation outperforms the best human effort at preventing rotation.

The images with data hidden using SELF hiding scheme also survive several other attacks included in *Stirmark*, e.g., Gaussian or median filtering, rows and/or columns removal, heavy JPEG compression, and aspect ratio change. The number of bits listed in Table 1 and 2 survive these attacks as well. Much less data can be hidden against the *Stirmark* random bending attack. For example, 73 bits are hidden in Peppers image (without the channel coding) and received with 20 % error. Note that this performance may still be good for watermarking applications, where the watermark sequence is known to the decoder and can be correlated with the hidden data to *detect* the watermark.

5. CONCLUSION

We have successfully demonstrated a print-scan resilient data hiding method with potential applications such as document authentication and image copyright protection. The robustness of the method is based on three key components of our approach: choice of embedding strategy based on coarse experimental modeling of the print-scan channel, the use of powerful channel codes, and an automated algorithm for derotation which specifically exploits printer halftoning algorithms. An important open question is whether it is possible to hide a significantly larger number of bits using still more sophisticated techniques. One possible approach is to employ information-theoretic techniques to estimate the capacity of print-scan resilient hiding; key to such an effort is more refined modeling of the print-scan process.

References

[1] K. Solanki, O. Dabeer, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Robust image-adaptive data hiding: Modeling, source coding and channel coding," in *42ed Annual Allerton Conf. on Communications, Control, and Computing*, Oct. 2003.

[2] J. K. O. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Processing*, vol. 66, no. 3, pp. 303–317, May 1998.

[3] C. Y. Lin and S. F. Chang, "Distortion modeling and invariant extraction for digital image print-and-scan process," in *Intl. Symp. on Multimedia Information Processing (ISMIP 99)*, Dec. 1999.

[4] V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain," *IEEE Trans. on Image Processing*, vol. 10, no. 11, pp. 1741–1753, Nov. 2001.

[5] P. Bas, J.-M. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Trans. on Image Processing*, vol. 11, no. 9, pp. 1014–1028, Sept. 2002.

[6] J. Rosen and B. Javidi, "Hidden images in halftone pictures," *Applied Optics*, vol. 40, no. 20, pp. 3346–3353, 2001.

[7] M. S. Fu and O. C. Au, "Data hiding watermarking in halftone images," *IEEE Trans. on Image Processing*, vol. 11, no. 4, pp. 477–484, Apr. 2002.

[8] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Proc. Workshop Information Hiding, IH'98, LNCS 1525, Springer-Verlag*, 1998, pp. 219–239.

[9] N. Jacobsen, K. Solanki, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Image adaptive high volume data hiding based on scalar quantization," in *Proc. IEEE Military Comm. Conf. (MILCOM)*, Anaheim, CA, USA, Oct. 2002.

[10] K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Robust image-adaptive data hiding based on erasure and error correction," Accepted for publication *IEEE Trans. on Image Processing*.

[11] D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for turbo-like codes," in *36th Allerton Conf. on Communications, Control, and Computing*, Sept. 1998, pp. 201–210.

[12] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. on Info. Theory*, vol. 47, no. 2, pp. 498–519, Feb. 2001.

[13] R. Ulichney, *Digital Halftoning*, The MIT Press, 1987.