# Modeling the Print-Scan Process for Resilient Data Hiding

Kaushal Solanki*, Upamanyu Madhow, Banglore S. Manjunath, and Shiv Chandrasekaran
*Department of Electrical and Computer Engineering*
*University of California at Santa Barbara,*
*Santa Barbara, CA 93106*

## Abstract

Print-scan resilient data hiding finds important applications in document security, and image copyright protection. In this paper, we build upon our previous work on print-scan resilient data hiding with the goal of providing a simple mathematical characterization for guiding the design of more sophisticated methods allowing higher volume of embedded data, or achieving more robustness. A model for print-scan process is proposed, which has three main components: a) effects due to mild cropping, b) colored high-frequency noise, and c) non-linear effects. It can be shown that cropping introduces unknown phase shift in the image spectrum. A new hiding method called Differential Quantization Index Modulation (DQIM) is proposed in which, information is hidden in the phase spectrum of images by quantizing the difference in phase of adjacent frequency locations. The unknown phase shift would get cancelled when the difference is taken. Using the proposed DQIM hiding in phase, we are able to survive the print-scan process with several hundred information bits hidden into the images.

**Keywords:** copyright protection, data-hiding, digital watermarking, document authentication, print-scan modeling.

## 1. INTRODUCTION

Growing concerns over security in the past few years make it necessary to develop strong deterrents against forgery of important documents such as passports, driving licences, and identification documents. Print-scan resilient data hiding provides a viable solution to this problem: security information (such as fingerprints, signature, or passport number) can be imperceptibly embedded into a picture in the document. Only specific devices, which have access to a secret key, can decode and authenticate the hidden information. Forgery of such documents become extremely difficult because the embedded data is inseparable from the picture.

The availability of new affordable devices (e.g., printers, scanners, and compact disc burners) and powerful software (e.g., image processing, and video editing software) have made it extremely easy for consumers to access, create, manipulate, copy, or exchange multimedia data. This has created an urgent need for protecting intellectual property in the digital media. Multimedia data hiding, defined as imperceptible embedding of information into a multimedia host, offers a potential solution, though with many challenges. Digital watermarking is a technology being developed, in which, copyright information is embedded into the host in a way that is robust to a variety of intentional or unintentional attacks. The ease with which images can be converted from print to digital form and vice versa makes it necessary that the embedded digital watermark is resilient to the print and scan operation.

Many pictures appear on magazines and newspapers everyday. With availability of inexpensive high resolution scanners, the image can be conveniently converted into a digital form and the ownership of the image may be claimed by someone else. To counter this, information can be hidden into these images before they are printed and the ownership can be verified in the digital format. A visible watermark would not be helpful in this case because it can be easily removed using any image processing software. With the availability of affordable digital cameras, more and more images are created in a digital form. The potential of e-commerce for digital images cannot be realized unless a system for owner identification is in place. In this scenario, it is desirable that the hidden ownership information does not get destroyed if the image is printed.

While it is very important for the embedded data to survive the print and scan process, it is a very complex and challenging problem. There has been a growing interest among researchers in this area, but little progress has been made because of the complex nature of the problem. One of the first approaches was by Lin and Chang,[1]

*Send correspondence to K. Solanki: solanki@ece.ucsb.edu



Security, Steganography, and Watermarking of Multimedia Contents VII, edited by Edward J. Delp III, Ping Wah Wong, Proc. of SPIE-IS&T Electronic Imaging, SPIE Vol. 5681 © 2005 SPIE and IS&T · 0277-786X/05/$15

who model the print-scan process by considering the pixel value and geometric distortions separately. There are some watermarking methods[2–4] that were not specifically designed for the print-scan attack, but they do report robustness against the print-scan operation under specified experimental setup. A few approaches focus on hiding in halftone images,[5,6] wherein, the halftone cells of the host image are shifted based on the data to be hidden, and a composite halftone image is given out directly. More recent related works include Voloshynovskiy et al,[7] Mikkilineni et al,[8] Picard et al,[9] and Mahmoud et al,[10] all of which deal with document security in general rather than specifically considering printing and scanning of digital images.

Most of the above methods embed only a single bit (or a few bits) of information, as they assume the availability of the watermark sequence at the decoder. In our recent work on print-scan resilient hiding,[11,12] an improvement over these methods is achieved in terms of volume of embedding. 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). The hidden images also survive several other attacks such as those included in *Stirmark*,[13] e.g., Gaussian or median filtering, scaling or aspect ratio change, heavy JPEG compression, rows and/or columns removal, and to a lesser extent, random bending. The proposed method, called selective embedding in low frequencies (SELF), is an image-adaptive technique based on experimental modeling of the print-scan process. A new method to estimate and undo rotation is also proposed, which specifically exploits the fact that laser printers use an ordered digital halftoning algorithm for printing.

In this paper, we build upon the above work with a view of gaining a better understanding of the print-scan process via a more refined mathematical model. With a better understanding of the channel, we hope to embed higher volumes of data using more sophisticated embedding strategies. We also aim to survive attacks such as cropping and scaling that may happen during the print-scan process. There are many printing and scanning technologies available, and their effect on the image would vary a lot. It may not be possible to construct a unified model for whole spectrum of printing and scanning devices available in the marketplace. Hence, in this paper, we focus only on laser printers and flatbed scanners.

Our print-scan model has three main components: mild cropping, correlated high-frequency noise, and non-linear effects. At the time of scanning, the image part must be cropped out from the background, either manually or automatically. At this point, some mild cropping of the image is inevitable. Empirical evidence indicates that even very mild cropping affects the image spectrum a lot, including the low frequency coefficients that we are interested in. High-frequency noise gets added to the image as a result of the digital halftoning and the printing process. This affects the high frequency spectrum of the image, so that the high frequency coefficients cannot be used for data embedding. Both printing and scanning processes introduce non-linearity, which includes the gamma correction that happens at the time of scanning.

We are more interested in the affect of the components of our models on the low frequency coefficients since our current SELF embedding scheme hides in these low frequency bands. We observe that cropping affects the low frequency coefficients the most, and hence, we consider it in more detail. A new method to survive cropping is proposed, whose design is guided by our analysis on the effect of cropping.

We show that mild cropping causes a phase shift in the frequency coefficients which is approximately same for neighboring frequencies. Based on this observation, a new hiding method is proposed in which, information is hidden in the phase spectrum of images by quantizing the difference in phase of adjacent frequency locations. The unknown phase shift caused due to cropping would get cancelled when the difference is taken. The idea of hiding in difference of adjacent locations is analogous to 'differential phase shift keying' (DPSK), used to combat the effect of unknown channel phase shifts in wireless communication. We employ similar nomenclature, and term the proposed method *differential quantization index modulation* (DQIM). Using the DQIM hiding in phase, we are able to survive the print-scan process with several hundred bits hidden into the images.

The rest of the paper is organized as follows. A brief background of the printing and scanning processes is provided in Section 2. Section 3 provides an overview of our previous work on print-scan resilient data hiding. In Section 4, we discuss our mathematical model, and a strategy to survive cropping in the context of print-scan resilient hiding is discussed in Section 5. A new embedding method to survive print-scan, the phase DQIM hiding, is described in Section 6. Finally, we present results in Section 7, and concluding remarks in Section 8.

## 2. BACKGROUND

In this section, we provide a brief background of the printing and scanning processes. An understanding of these processes would give us some insights on construction of an underlying model.

### 2.1. The Printing Process

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[14] for an extensive discussion on halftoning methods.

The printer resolution, specified in dots per inch (dpi), need not be equal to the number of pixels per inch to be printed for an image. One can specify the number of pixels per inch for an image, which eventually determines the number of dots that will be printed for every pixel of the image. For example, if we set the image to be printed at 60 pixels per inch, and set the printer resolution at 600 dpi, then a square of $10\times10$ dots will be dedicated to a pixel of the printed image. The quality of the printed image depends on the type and age of the printer, as well as the status of the toner.

### 2.2. The Scanning Process

In a scanner, the picture to be scanned is illuminated and the reflected intensity is then converted into electrical signal by a sensor, which is then digitized. The scanning procedure involves putting the picture to be scanned on the scanner flatbed. The picture may undergo a mild rotation if it is not placed well on the flatbed. This rotation is generally limited to a few degrees (3 degrees or less) since the corner of the picture to be scanned can be aligned with the corner of the flatbed with a good accuracy. The scanning software allows one to set the resolution at which the picture is to be scanned. This resolution may vary from 75 dpi to 1200 dpi or more. The resolution determines the number of pixels scanned per inch of the document.

Another significant process that happens during the scanning is the *gamma correction*. Images are scanned into a computer for display on a monitor and for storage in digital media. Every computer monitor has an intensity to voltage response curve which is a power function with parameter $\gamma$. This means that if we send a computer monitor a message that a certain pixel should have intensity equal to $x \in (0, 1)$, it will actually display a pixel which has intensity equal to $x^\gamma$. Most monitors have a gamma of roughly 2.2, which means that the intensity value displayed will be less than what we wanted it to be. In order that the scanned image is correctly displayed on a monitor, the image data generated at the scanner is 'gamma corrected' (ie raised to a power $1/\gamma$). The scanner software allows users to set the gamma correction that is to be applied for an image (the default being 2.2).

## 3. PRINT-SCAN RESILIENT DATA HIDING

In this section, we provide an overview of our previous work on print-scan resilient data hiding (see[11] for details). This method is based on experimental modeling of the print-scan process, as described below. Focussing on laser printers, a method to estimate and undo rotation that might happen during the scanning process is also proposed.

### 3.1. Experiments and Observations

We printed and scanned several grayscale images using commercially available printer and scanner. 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. 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. Some interesting trends in the DFT coefficient magnitudes were discovered, as listed below.

[†]Some modern printers allow for more levels, but still require halftoning. Such printers are not used in our experiments and hence not considered here.

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.

The observations made above form the basis of the embedding scheme described in the following section. These observations will be later explained in terms of the mathematical model proposed in Section 4.

### 3.2. Selective Embedding in Low Frequencies

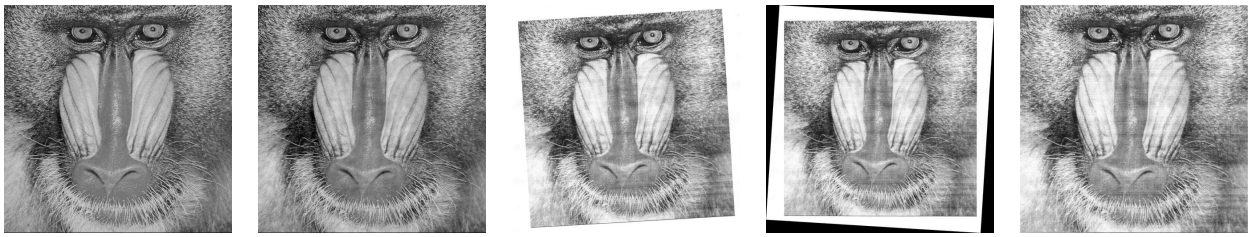
Based on the experimental modeling described in the previous section, we propose a new image-adaptive hiding method that achieves robustness against the print-scan operation. Information is hidden only in dynamically selected low frequency coefficients whose magnitude is greater than a predefined threshold.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

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). 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 coding framework was first employed in our previous work on robust image-adaptive data hiding.[15] 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.

### 3.3. Estimating and Undoing Rotation

A method to estimate and undo rotation that might happen during the scanning process is proposed, which specifically uses the knowledge of printer halftoning algorithm. We limit our attention to laser printers in this paper, which employ an ordered halftoning algorithm to generate the binary image. The halftone pattern can be captured by high resolution scanning and can be used to estimate and undo rotation. The rotation angle 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 shows the images at some of these intermediate stages. Figure 1 (a) and (b) show the original image and the composite image with 475 bits embedded. Figure 1 (c) shows the printed-and-scanned image which has been rotated during the scanning process. Figure 1 (d) shows the automatically derotated image (step (3)). Figure 1 (e) shows the image after the background is automatically cropped (step (4)).



(a) Original 512×512 Baboon image

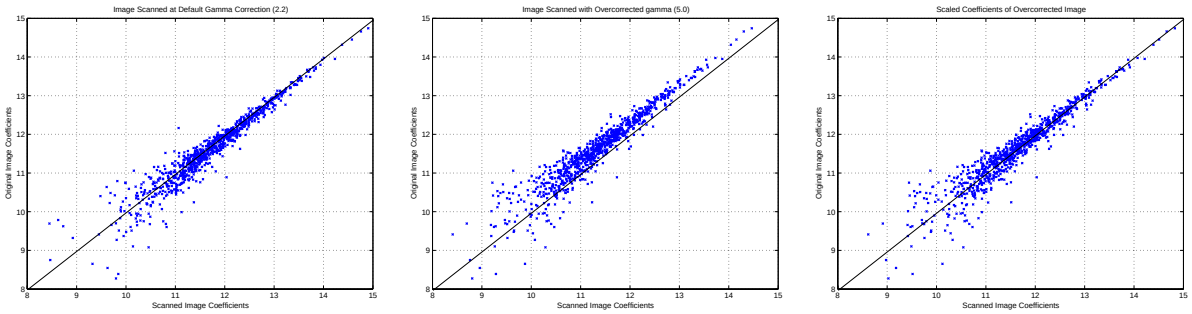
(b) Image with 475 bits hidden

(c) Printed and scanned image

(d) Automatically derotated image

(e) The derotated image cropped automatically

**Figure 1.** Images at various stages of embedding, attack, and decoding.




(a) Image scanned with a gamma correction of 2.2.

(b) Image scanned with a gamma correction of 5.0 (overcorrection).

(c) The coefficients of the overcorrected scanned image of (b) are scaled by 1.023.

**Figure 2.** Effect of gamma correction: Logarithm of low frequency DFT coefficient magnitudes of original 512×512 peppers image are plotted against those of the same image after printing and scanning. $1/N^2$ scaling has not been applied in computing the DFT. It can be seen that the plot is spread around the x=y line for the gamma correction of (a). If the image is overcorrected at the scanner (b), the response shifts. However, a plot spread around x=y can be achieved by scaling of the coefficients (c).

### 3.4. Undoing Incorrect Gamma Correction

When the printout of an image is scanned, it undergoes gamma-correction, as discussed in Section 2.2. Different computer systems may have different system gamma (e.g., Macintosh computers use a gamma of 1.8, while the gamma for PCs vary from 2.2 to 2.5) and it is important to apply the right gamma correction at the receiver. We experimented with various gamma correction values at the scanner in order to find a way to deal with incorrect gamma correction. As in all previous experiments, we study the logarithm of DFT coefficient magnitudes here.

In the experiments, we observed that when the gamma correction is varied at the scanner, the logarithm of DFT coefficient magnitudes of the scanned image are scaled by a constant factor. Figure 2 plots the original and scanned image DFT coefficients (or the *input/output* characteristics) for the default gamma correction (monitor gamma = 2.2) and for overcorrection (monitor gamma = 5.0). Figure 2 (c) shows the same plot when the scanned image DFT coefficient magnitudes are scaled. It can be seen that the plot in (c) is quite close to the unity gain line. The gamma correction applied, in general, depends on the system gamma. Thus, we can deal with incorrect gamma correction that may happen during scanning simply by scaling the log DFT coefficient magnitudes.

## 4. MODELING THE PRINT-SCAN CHANNEL

Printing followed by scanning involves conversion of from digital to analog, and back to digital form. This is inherently a very complex process. The problem is compounded by the fact that a variety of printing and scanning devices are available in the market, which work on one of many existing technologies. Obviously, constructing a unified model will be extremely difficult, if not impossible. Hence, we limit ourselves to laser printers and flatbed scanners.

Even when only laser printers and flatbed scanners are considered, constructing a complete or near complete model would require so many parameters that the resulting model will no longer remain very useful practically. Hence, we focus on constructing a model which is quite simple, yet more refined than a completely empirical model stated in Section 3. We use the observations made in Section 3.1 to guide the construction of the proposed model. More experiments have been carried out to validate the model and also learn the parameters involved.

As stated in Section 1, there are three components of our print-scan model, namely, mild cropping, high-frequency noise, and non-linear effects. All these components are actually quite broad in their definition, and can be thought of as sub-processes that constitutes the print-and-scan process as a whole. We now describe the individual components of our model in more detail (Sections 4.1 - 4.3). After describing the individual components, we shall discuss some issues regarding the model in Section 4.4.

### 4.1. Mild Cropping

Some mild cropping is inevitable during the scanning process, when the image is cropped from the background either manually or automatically. As a result, the effects due to cropping cannot be ignored in the design of a print-scan resilient hiding method.

Consider an image $f(n_1, n_2)$ with $N_1$ rows and $N_2$ columns, so that it is defined over the domain $\Omega = \{0, 1, 2, ..., N_1 - 1\} \times \{0, 1, 2, ..., N_2 - 1\}$. Cropping of the image can be thought of as a multiplication with a masking window. Assuming that the image is cropped to new dimensions of $M_1 \times M_2$ (with $M_1 \leq N_1$, and $M_2 \leq N_2$), the masking window $r(n_1, n_2)$, also defined over $\Omega$, can be written as,

$$r(n_1, n_2) = \begin{cases} 1 & \text{if } M_{1a} \leq n_1 < M_{1b}, \text{ and } M_{2a} \leq n_2 < M_{2b}, \\ 0 & \text{otherwise.} \end{cases}$$

Note that $M_{1a}$ and $M_{1b}$ define the top and bottom cropping locations respectively, so that $M_1 = M_{1b} - M_{1a}$. Likewise, $M_2 = M_{2b} - M_{2a}$. We can now define the cropped image $c(n_1, n_2)$ as,

$$c(n_1, n_2) = f(n_1, n_2) \times r(n_1, n_2) \qquad \forall \{n_1, n_2\} \in \Omega$$

This product is equivalent to circular convolution in the DFT domain. Defining $F(k_1, k_2)$, $R(k_1, k_2)$, and $C(k_1, k_2)$ as the 2D DFT of $f(n_1, n_2)$, $r(n_1, n_2)$, and $c(n_1, n_2)$ respectively, the circular convolution can be written as,

$$C(k_1, k_2) = \sum_{l_1=0}^{N_1-1} \sum_{l_2=0}^{N_2-1} F(l_1, l_2) \cdot R(\langle k_1 - l_1 \rangle_{N_1}, \langle k_2 - l_2 \rangle_{N_2})$$

Here, $\langle \cdot \rangle_N$ denotes the modulo $N$ operator. The DFT of the masking window $r(n_1, n_2)$ would be a sinc-like function[‡], with its shape being a function of $M_1$ and $M_2$, and a phase shift that depends on the location of the masking window, i.e., $M_{1a}$ and $M_{2a}$. When the cropping is mild, $N_1 - M_1$ and $N_2 - M_2$ are small, and the sinc-like function would be quite *narrow*. For mild cropping, most of the energy of $R(k_1, k_2)$ is concentrated on the $\{0, 0\}$ coefficient, along with low frequency part of the first row and first column. Thus, the blurring of the original image spectrum will be mild for those DFT coefficients whose magnitude is high or of the same order as its neighbors. However, for coefficients whose magnitude is significantly lower than its neighbors, the blurring will cause its magnitude to increase. This will affect low magnitude coefficients in all the frequency bands -

[‡]Note that $R(k_1, k_2)$ is a discrete function, which does not strictly follow the sinc definition. It still has a shape similar to the sinc function, and hence we call it *sinc-like*.

high, mid, or low. This inference is also validated by empirical observations listed in Section 3.1. Specifically, this explains the *observation 2*, which states that the low magnitude coefficients see a higher noise than the high magnitude ones. In Section 5, we consider the possible strategies to survive cropping.

### 4.2. Colored High Frequency Noise

Before an image is printed, it is converted into a digital halftone, as stated in Section 2.1. Digital halftoning algorithms tend to put the quantization noise in high frequencies[14] since the human visual system is not very sensitive to high-frequency noise. This introduces high-frequency noise into the image. Another source of colored noise is the printing process itself. Uncertainties during the printing operation adds correlated noise which varies every time a printout is taken.

Addition of the high-frequency noise heavily affects the high frequency DFT coefficients. Due to this reason, the high-frequency coefficients are not appropriate for embedding data. This is consistent with the *observation 1* made in Section 3.1, which says that low and mid frequency coefficients are preserved much better than the high frequency ones. The affect of this component of our model is mostly limited to high and mid frequency coefficients. It is observed that in the mid, or sometimes low frequency bands, the noise specifically affects the low magnitude coefficients. Since we are more interested in the affects on low frequency bands, we do not analyze this component in more detail here. Such an analysis would be an interesting avenue for the future work.

### 4.3. Non-linear Effects

Images are scanned into a computer for display on a monitor and for storage in digital media. Every computer monitor has an intensity to voltage response curve which is a power function with parameter $\gamma$. As described in Section 2.2, in order that the scanned image is correctly displayed on a monitor, the image data generated at the scanner is 'gamma corrected' (ie raised to a power $1/\gamma$). When considering an end-to-end system, this process invariably introduces non-linear transformation.

Note that in their model, Lin and Chang[1] propose a responsivity function to take into account the AC, DC and gamma adjustments. The proposed function has four independent parameters and a pixel dependent noise term. The complexity of this model would not make it useful in the current context. The main thrust of the present work is to come up with a simple model for the print-scan process that would enable us to hide information into images resilient to the print-scan operation. As before, we are interested in the low frequency DFT coefficients. We observe that these non-linear transformation effects the mid and high-frequency coefficients as well as the low magnitude coefficients in the low frequency bands. This is again consistent with *observation 2* made in Section 3.1, which states that low magnitude coefficients see a much higher noise then their neighbors with higher magnitude.

### 4.4. Discussion

An interesting point to note is that out of all above components, only cropping contributes to distortion in all the frequency bands equally. The other two components tend to affect mid and high frequency coefficients more than the low frequency ones. Since we are more interested in data hiding in the low frequency bands, effect of cropping becomes more significant. In their model, Lin and Chang[1] also consider cropping to be an important factor. They view it as an additional source of noise. Moulin and Briassouli[16] consider cropping as well, although not in the context of print-scan. Similar to our observation, they view cropping as causing blurring in the frequency domain.

Note that cropping is not a "natural" process that happens during the printing and scanning operation, since, neither the printer nor the scanner actually causes cropping. Hence, including it in a print-scan model might be arguable to some readers. Our reason for including cropping in the model is that it can never be completely separated from the print-scan process, at least for blind decoding. Analyzing cropping in the context of print-scan becomes more important because it is the biggest contributor of distortion in the low frequency bands. One more point to note is that, in general, it is very difficult to achieve perfect registration between the original and the attacked image due to presence of cropping, however mild. When the images are analyzed, this imperfect registration might be the reason for observation of higher noise near the edges within the image.

Instead of specifically modeling this noise, we find it more appropriate to consider mild cropping separately, and not worry about the registration issue.

In the print-scan model proposed by Lin and Chang,[1] blurring of the image has been considered via a couple of point spread functions. Voloshynovskiy et al[7] also view the printing process as causing blurring of the image. The main reason for these authors to consider image blurring is that digital halftoning introduces low pass filtering of the image as understood in the inverse halftoning literature (see[17] for a survey of inverse halftoning). However, we have not incorporated image blurring in the current proposal of the print-scan model. There are two main reasons. First, in the printing scenario we consider, the images were printed at high resolution. Several dots are dedicated to one pixel, e.g., when a 512×512 image is printed (at 600 dpi printer resolution) on an *letter* paper with 72 pixels per inch, the size of the image on the paper is 7.11"×7.11". In this case, it turns out that on an average, a block of 8.33×8.33 dots is used for every pixel of the image. At this resolution, the image does not get blurred during the printing process. The second reason is that we are using laser printers in our experiments. The image blurring is often observed with inkjet printers at lower resolutions, as reported in.[1]

## 5. SURVIVING CROPPING

Cropping appears to be the most significant impairment for the low frequency coefficients that we hide data in. Hence, we consider it in more detail here. Usually, the amount of cropping performed as well as the location of the cropping window is not known to the decoder. Following the notation of Section 4.1, while $M_1$ and $M_2$ define the size of the masking window $r(n_1, n_2)$, the location of the masking rectangle is determined by $M_{1a}$ and $M_{2a}$.

Let us first consider the scenario where the percentage of cropping is known (i.e., $M_1$ and $M_2$ are known), but its location in the original image is not known (i.e., $M_{1a}$ and $M_{2a}$ are not known). In this case, the rectangular mask has known dimension, but there is an unknown offset. In the frequency domain, the 2D DFT, $R(k_1, k_2)$ will be a two dimensional sinc-like function which has known magnitude spectrum (or the "shape"), but unknown phase. As stated previously, for mild cropping, the rectangular mask is large, so that this sinc-like function is quite narrow. This causes mild blurring of the spectrum, which can be ignored for high magnitude coefficients. When the cropping is not very mild, we must explicitly or implicitly take the blurring of the image spectrum into account.

We now construct a simple hiding strategy that can potentially survive a predetermined maximum level of cropping. The idea is to take into account the affect of cropping at the encoder, so as to modify a specific DFT coefficient of the host image in such a manner that after cropping, this coefficient would be closer to reconstruction point of either the '0', or the '1' quantizer depending on the bit hidden.

Consider an image $f(n_1, n_2)$, whose DFT is given by $F(k_1, k_2)$. Now, let us crop the image to the maximum level (i.e., minimum permissible $M_1$ and $M_2$), at any location using the rectangular window $r(n_1, n_2)$ whose DFT is given by $R(k_1, k_2)$. Let us denote this cropped image by $c(n_1, n_2)$ and its DFT by $C(k_1, k_2)$. Note that this $C(k_1, k_2)$ is one particular instance of the blurring of $F(k_1, k_2)$ due to cropping. When the cropping is not very severe (e.g., more that 50% by area), we assume that the blurring causes similar overall effect to the coefficients. There will be additional noise due to the variation of actual location of the cropping window. We try to estimate this overall effect using this one particular instance and then use this knowledge to embed information. In practice, we observed that this estimate is good only for those coefficients, whose magnitude is higher than its neighbors.

Let us choose a particular coefficient $F_i = F(x, y)$ in the low frequency band to embed binary information. Likewise, the same coefficient $C(x, y)$ is denoted by $C_i$ for simplicity. Also, denote the DC coefficient of the spectrum of the masking window by $R_{dc} = R(0, 0)$. Since the spectrum $C(k_1, k_2)$ can be given by the circular convolution of $F(k_1, k_2)$ and $R(k_1, k_2)$, we have,

$$C_i = R_{dc} F_i + \text{other terms}$$

Since we know $C_i$, $R_{dc}$ and $F_i$, we can compute an estimate of the sum of all other terms as $C_i - R_{dc} F_i$. Now, in order to hide a bit $b \in \{0, 1\}$, we want that the new cropped image coefficient $C_o$ to be a quantized version of

$C_i$. That is, we want that $C_o = Q_b(C_i)$ by modifying $F_i$ to $F_o$. Here we get,

$$C_o = R_{dc}F_o + C_i - R_{dc}F_i$$

After some simplifications, we get,

$$F_o = F_i + \frac{C_o - C_i}{R_{dc}}$$

Note that $R_{dc}$ is always less than 1, and hence, the above equation indicates that the change we have to make to the host image coefficient is a factor of $1/R_{dc}$ more than the change we observe in the same coefficient in the cropped image. The $F_o$ we would observe after actual cropping may vary from the one projected here because the location of the masking window in actual attack may vary from the one used here. As stated before, the assumption that the affect would be similar for different crop window locations is valid only when the magnitude of the coefficient under consideration is high. Hence, we modify the embedding strategy to make sure that the magnitude of the modified coefficient is always higher than the original one (i.e, $F_o > F_i$). This is done by choosing only those quantizer reconstruction points which are greater than the present value (though this might cause a larger distortion). Also, note that, as in the rest of the paper, we modify the logarithm of the magnitude of the coefficients. We present the preliminary results of this embedding strategy in Section 7. As in the formulation above, we embed only a single bit of information in the image. Some potential strategies to enable us to hide larger number of bits are currently under investigation.

It should be noted that the proposed crop-resilient embedding scheme is still limited by the fact that the decoder must know the amount of cropping, i.e., the variables $M_1$ and $M_2$. We concede that this would be a major limitation in case of cropping that happens digitally. However, in case of print-scan resilient hiding, there is a simple way to compute the amount of cropping at the decoder. Here, we can use the printer halftone pattern to estimate the number of *original* pixels contained in the received image. Note that we have used the printer halftoning algorithm to estimate and undo rotation that might happen during the scanning process (See Section 3.3). A similar approach to estimate the amount of cropping after scanning is currently under investigation. We now turn our attention to a new hiding method for the phase spectrum, as described in the following section.

## 6. DIFFERENTIAL QUANTIZATION INDEX MODULATION

Quantization index modulation (QIM), proposed by Chen and Wornell,[18] are a class of information hiding methods, in which data is embedded into the host sample by the choice of quantizer. We propose an extension to this method with the goal of surviving the cropping and the print-scan processes. Instead of just quantizing the host signal, we embed data by quantizing the difference of two adjacent host samples. The idea of hiding in difference of adjacent locations is analogous to 'differential phase shift keying' (DPSK), used to combat the effect of unknown channel phase shifts in wireless communication. We employ similar nomenclature, and term the proposed method *differential quantization index modulation* (DQIM).

We use DQIM to embed information in the phase spectrum of the images to counter unknown phase shift induced due to mild cropping. As discussed in Section 4.1, cropping is equivalent to circular convolution of the image spectrum with a narrow sinc-like function. Let us focus only on mild cropping, where the sinc-like function, $R(k_1, k_2)$, is quite narrow. If we look only at low frequency coefficients, and assume that the particular DFT coefficient under consideration does not have significantly low magnitude compared to its neighbors, we have only two dominant terms in the convolution expression,

$$C(k_1, k_2) = R(0,0) \cdot F(k_1, k_2) + R(k_1, k_2) \cdot F(0,0) + \text{other terms}$$

In the above expression, while the first term would not cause a phase shift, the second term would. This would depend on the phase of $R(k_1, k_2)$ itself. Since the phase of the sinc-like $R(k_1, k_2)$ varies slowly, the phase spectrum of $C(k_1, k_2)$ would have a slowly varying phase shift with respect to $F(k_1, k_2)$. Note that the phase of $R(k_1, k_2)$ varies slowly except for the zeros of the sinc where the variation in phase is larger. However, for mild cropping, the number of such zeros would be very few.

In the actual implementation, we scan the image phase spectrum row-wise. Note that only those coefficients that lie in a predefined band are used for embedding information. Let us denote the row-wise scanned original

image phase values by $\phi_n$, where $n$ is the index ($n \in \{0, 1, 2, ..., N_{max}\}$), and the quantized values by $\theta_n$. Then, the embedding function is,

$$\theta_n = \langle Q_b(\phi_n - \theta_{n-1}) \rangle_{2\pi} \forall n \in \{1, 2, ..., N_{max}\}$$

Note that since we are dealing with phase, we must output the modulo-$2\pi$ values after the quantization $Q_b(\cdot)$ of the difference is done. Also note that we use the quantized values $\theta_n$ to compute the phase difference for the next coefficient. This is done to maintain consistency for the decoder, which just finds these differences, and determines which of the two quantizers was used.

As discussed before, the assumption of slowly varying phase shift is not valid for those coefficients whose magnitude is significantly lower than it neighbors. Hence, we avoid hiding in these locations, and use turbolike repeat-accumulate (RA) codes to counter the synchronization problem caused due to adaptive hiding.[11, 15] The use of coding framework to counter insertions/deletions problem has also been discussed briefly in Section 3.2.

## 7. RESULTS

In order to verify the validity of the proposed model, we construct an example where, a dummy printed and scanned image is constructed using a simulated attack. We compare this with the same image after actual print-and-scan operation. Figure 3 (a) and (b) shows the simulated and actual images respectively. The images look very similar perceptually, although the finer details may not be visible in the displayed images. The similarity is maintained in the transform domain as well. Figure 3 (c) and (d) show the low frequency DFT magnitude spectra of the two images. The coefficients are quite close to each other, with few notable exceptions. Though only one specific example is presented here, similar observations have been made for all the test images.

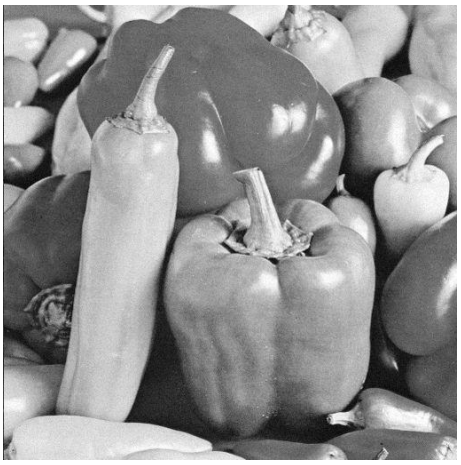
We believe that a visual examination, like the one presented above, is necessary to show the goodness of the presented model. However, by itself, this is not sufficient to validate the model. More experimental and mathematical analysis would be required to make concrete claims. We present this example just to show that the proposed coarse modeling may be a good starting point to guide the design of simple print-scan resilient hiding methods.

We evaluated the performance of the embedding scheme of Section 5, which is designed to survive cropping. In the preliminary results presented here, we embed one bit of information in a single DFT coefficient of the host image. As an example, we choose the $(6, 6)$ coefficient of the 512×512 'fishing boat' image to embed the bit. The maximum cropping is a design parameter, which is set to 100 rows/columns in both directions (i.e., $M_1 = M_2 = 412$), which amounts to cropping more than a third of the image by area. The hidden bit is recovered from the composite image after it has been cropped severely, up to the design maximum. No errors were observed in a number of runs that were carried out with varying locations of the cropping window.

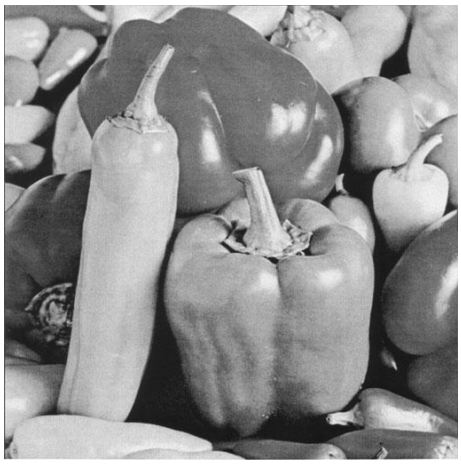
For our DQIM hiding in phase method, we are able to embed several bits against the print-scan attack. The volume of embedding depends on the host image. When compared to the SELF hiding scheme for hiding in magnitudes, the volume of embedding is slightly less. As an example, we can embed 125 bits into 512×512 peppers image using the DQIM hiding with perfect recovery after the print-scan attack. The 125 bits to be embedded are coded using rate 1/5 RA code, so as to get a stream of 625 bits. These bits are embedded into the low frequency DFT coefficients of the host image. In this example, the low frequency band spans 576 coefficients. Data is hidden into a coefficient in this band only if its magnitude is greater than a predefined threshold, and the corresponding code symbol is erased at the encoder. Since we are using DQIM, if a coefficient does not pass the threshold test, the next one is also skipped.

## 8. CONCLUSION

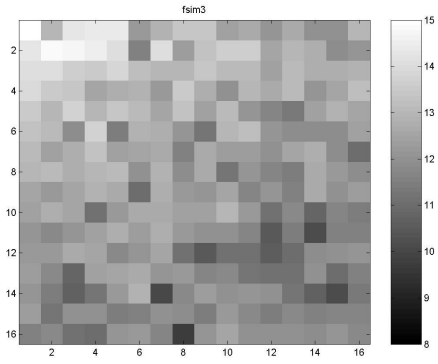
In this paper, we propose a mathematical characterization of the print-scan process by dividing it into three sub processes. Our main focus here is to create a simple and practical model that can be used to guide design of data hiding schemes that survive the print-scan process. The model does inspire construction of two new embedding strategies proposed in this paper: a technique to survive cropping by estimating its effect beforehand, and a method to survive the print-scan process by DQIM embedding in the phase spectrum. While the proposed model does sound promising, much more work needs to be done to completely validate it.



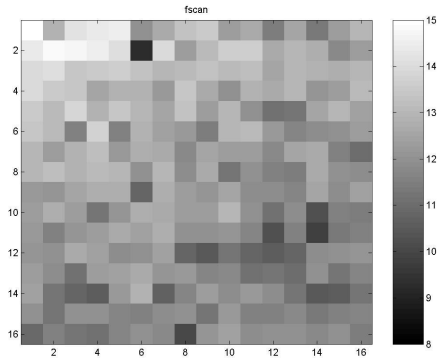
(a) Simulated attack



(b) Actual print-scan attack




(c) Low-frequency magnitude spectrum of simulated image




(d) Low-frequency magnitude spectrum of actual attacked image

**Figure 3.** Image with simulated print-scan attack as compared to actually printed and scanned image.

## Acknowledgement

This research is supported in part by a grant from ONR # N00014-01-1-0380.

## REFERENCES

1. 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*, Dec. 1999.
2. J. K. O. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Processing* **66**, pp. 303–317, May 1998.
3. V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain," *IEEE Trans. on Image Processing* **10**, pp. 1741–1753, Nov. 2001.
4. P. Bas, J.-M. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Trans. on Image Processing* **11**, pp. 1014–1028, Sept. 2002.
5. J. Rosen and B. Javidi, "Hidden images in halftone pictures," *Applied Optics* **40**(20), pp. 3346–3353, 2001.

6. M. S. Fu and O. C. Au, "Data hiding watermarking in halftone images," *IEEE Trans. on Image Processing* **11**, pp. 477–484, Apr. 2002.
7. S. V. Voloshynovskiy, O. Koval, F. Deguillaume, and T. Pun, "Visual communications with side information via distributed printing channels: extended multimedia and security perspectives," in *Proc. of SPIE: Security, Steganography, and Watermarking of Multimedia Contents VI*, pp. 428–445, (San Jose, CA, USA), Jan. 2004.
8. A. K. Mikkilineni, G. N. Ali, P.-J. Chiang, G. T. C. Chiu, J. P. Allebach, and E. J. Delp, "Signature-embedding in printed documents for security and forensic applications," in *Proc. of SPIE: Security, Steganography, and Watermarking of Multimedia Contents VI*, pp. 455–466, (San Jose, CA, USA), Jan. 2004.
9. J. Picard, C. Vielhauer, and N. Thorwirth, "Towards fraud-proof ID documents using multiple data hiding technologies and biometrics," in *Proc. of SPIE: Security, Steganography, and Watermarking of Multimedia Contents VI*, pp. 416–427, (San Jose, CA, USA), Jan. 2004.
10. K. W. Mahmoud, J. M. Blackledge, S. Datta, and J. A. Flint, "Print protection using high-frequency fractal noise," in *Proc. of SPIE: Security, Steganography, and Watermarking of Multimedia Contents VI*, pp. 446–454, (San Jose, CA, USA), Jan. 2004.
11. K. Solanki, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Estimating and undoing rotation for print-scan resilient data hiding," in *Proc. ICIP*, (Singapore), Oct. 2004.
12. 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.
13. 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*, pp. 219–239, 1998.
14. R. Ulichney, *Digital Halftoning*, The MIT Press, 1987.
15. K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Robust image-adaptive data hiding based on erasure and error correction," *IEEE Trans. on Image Processing* **13**, pp. 1627 –1639, Dec 2004.
16. P. Moulin and A. Briassouli, "A stochastic QIM algorithm for robust, undetectable image watermarking," in *Proc. ICIP*, (Singapore), Oct. 2004.
17. M. Mese and P. P. Vaidyanathan, "Recent advances in digital halftoning and inverse halftoning methods," *IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications* **49**, pp. 790–805, June 2002.
18. B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Trans. on Info. Theory* **47**, pp. 1423–1443, May 2001.