Document Identification for Copyright Protection Using Centroid Detection

Steven H. Low, *Member, IEEE,* Nicholas F. Maxemchuk, *Fellow, IEEE,* and Aleta M. Lapone

***Abstract*— A way to discourage illicit reproduction of copyrighted or sensitive documents is to watermark each copy before distribution. A unique mark is embedded in the text whose recipient is registered. The mark can be extracted from a possibly noisy illicit copy, identifying the registered recipient. Most image marking techniques are vulnerable to binarization attack and, hence, not suitable for text marking. We propose a different approach where a text document is marked by shifting certain text lines slightly up or down or words slightly left or right from their original positions. The shifting pattern constitutes the mark and is different on different copies. In this paper we develop and evaluate a method to detect such minute shifts. We describe a marking and identification prototype that implements the proposed method. We present preliminary experimental results which suggest that centroid detection performs remarkably well on line shifts even in the presence of severe distortions introduced by printing, photocopying, scanning, and facsimile transmission.**

***Index Terms*— Centroid detection, centroid noise, document marking, image processing copyright, text watermarking.**

I. Introduction

An IMPORTANT application of future communications networks will be electronic publishing and digital library, provided copyright can be protected. A way to discourage illicit reproduction of copyrighted or sensitive documents is to watermark the document before distribution. A unique mark is permanently embedded in the document and its recipient is registered. The mark must be indiscernible, yet it must survive common processes a document might be subjected to, such as printing, photocopying, scanning, and facsimile transmission, so that it can be detected from a noisy illicit copy to identify the original recipient. We have prototyped such a system. Preliminary experimental results show that very reliable identification can be achieved in the presence of severe distortions introduced by such processes. This paper presents one of the two detection techniques used in our system.

Watermarking methods have been proposed to discourage illicit reproduction of picture and video images in [23], [1], [15], [24], [9], [10], [5], [14], [7], [22], [21], and [8], but these techniques either are not directly applicable to or do not exploit the regular structure of text documents. Moreover, most image marking techniques are ideal to mark images with rich grayscale and may not be well-suited for binary images, such as a text image, since slight perturbation of image intensity can easily be removed by binarization. In [6] a cryptographic system for the secure distribution of electronic documents is described. In [3] the approach to indiscernibly mark each document copy by varying the line or word spacing or by varying certain character features slightly is proposed. In [13] an experiment is reported which reveals that a document can be distorted much more severely in one direction than the other, and a marking and identification strategy that exploits this difference is described. The detection scheme reported in this paper is more sophisticated than those in [3] and [13]. In [2] several ways to assign unique identifiers to copies of digital data are studied that are secure against collusion among recipients to detect and remove the marking.

We mark a page of text by shifting certain lines slightly up or down from their normal positions or certain words slightly left or right. The shifting pattern constitutes the mark and is different on different copies.

To detect line shifts, the horizontal profile of lines is compiled from a digitized image of the page. These profiles are commonly used in computer analysis of structural document layouts [19], [18], [17]. A typical horizontal profile consists of distinct tall and narrow columns. This suggests the approximation of each such column by a delta function situated at the column's centroid. Marking shifts these centroids (delta functions) while document processing adds noise to the profile and perturbs these centroids randomly. Marks are detected by comparing the centroids of the original unmarked profile with those of its noisy marked copy.

Word shifts can be detected by a similar procedure. As to be shown in the sequel, however, detection error for word shifts is significantly larger than that for line shifts using centroid detection. This has led to the development of a different method to detect word shifts; see [12] for details and comparison of these two methods.

In Section II we define formally a profile and propose a simple noise model to model how a horizontal or vertical profile is corrupted by printing, photocopying, scanning, and other processing.

In order to derive the maximum-likelihood detector for the centroid method, we characterize in Section III the effect of additive profile noise on the centroid positions. The major conclusion of that section is that, for typical profiles, if the

Paper approved by M. R. Civanlar, the Editor for Image Processing of the IEEE Communications Society. Manuscript received June 7, 1996; revised September 4, 1997. This paper was presented in part at GLOBECOM'95, Singapore, November 1995.

S. H. Low is with the Department of Electrical and Electronic Engineering, University of Melbourne, Parkville, Victoria 3052, Australia (e-mail: slow@ee.mu.oz.au).

N. F. Maxemchuk is with AT&T Laboratories—Research, Florham Park, NJ 07932 USA (e-mail: nfm@research.att.com).

A. M. Lapone is with Bell Laboratories, Lucent Technologies, Murray Hill, NJ 07974 USA (e-mail: amg@bell-labs.com).

Publisher Item Identifier S 0090-6778(98)02125-4.

additive profile noise is white Gaussian, then the centroid noise is approximately zero-mean Gaussian whose variance depends on the structure of the original unmarked profile and is easily computable. This is arrived in three steps. We first derive the exact density function of centroid noise. The exact density depends on the original unmarked profile as well as on the variance of the additive profile noise. It is, however, too complicated to be used for detection. Making use of characteristics of typical unmarked profiles, we then derive a remarkably simple Gaussian approximation to the exact density. Finally we justify the approximation by sketching its error bounds. Real document profiles are used to demonstrate the accuracy of this approximation. The approximation allows us to derive in Section IV the maximum-likelihood detector for the centroid method and its error probability.

We present in Section V some experimental results which show that centroid detection of lines shifts performs remarkably well in the presence of noise, but that of word shifts is much worse. This empirical observation can be explained qualitatively by the analytical result in Section IV. We briefly describe a marking and identification prototype that implements the proposed algorithm for line shift detection and another algorithm [12] for word shift detection.

We now comment on the applicability of the proposed technique. Different techniques are suited for watermarking different media such as music, video, pictures (paintings and photographics), and text. The proposed technique caters only for the watermarking of *formatted* text documents. Marks placed in a text, using *any* technique including the proposed one, can always be removed by retyping the document. A large part of this effort may be automated by character recognition devices. Alternatively, the marks can be concealed by dithering the positions that contain information by larger amounts than the encoder uses to enter the information. In contrast, marks placed in pictures or speech are assumed to be indelible. The ability to remove text marks limits its applications. Text marking is well suited for protecting modestly priced documents, such as newspaper or magazine articles. We assume that if legal and illegal copies are distinguishable (a document with markings altered or removed can be easily identified to be illicit), and legal copies are affordable, then most people will not seek out illegal copies.

Attacks on the proposed text marking method are further elaborated in [3]. Countermeasures can be devised to make the distortion needed to conceal marks intolerable, to make it difficult to forge valid marks, and to make the marks more difficult to remove; see [16] for details. For example, a publisher may watermark a document in postscript, but distribute marked copies in bitmap or paper. Then the marking process takes much less time than applying typical image marking techniques on bitmap images of the text and can be performed in real-time before distribution. Moreover, for the recipients, it will be difficult to remove the marks and more expensive to redistribute the illicit copies.

Throughout the paper $h(y)$ denotes an original unmarked and uncorrupted profile and $g(y)$ denotes its corrupted copy, marked or unmarked. By "$X := Y$" or "$Y =: X$" we mean "X is defined as Y."

II. Profile and Noise Models

A. Profiles and Marking

Upon digitization, the image of a page is represented by a function

$$f(x,y) \in [0,1], \qquad x = 0,1,\cdots,W, \quad y = 0,1,\cdots,L$$

that represents the grayscale at position (x,y). Here, W and L, whose values depend on the scanning resolution, are the width and length of the page, respectively. The image of a text line is simply the function restricted to the region of the text line

$$f(x,y) \in [0,1], \qquad x = 0,1,\cdots,W, \quad y = t, t+1,\cdots,b$$

where t and b are the top and bottom "boundaries" of the text line, respectively. For instance, we may take t or b to be the midpoint of the interline spacing. The *horizontal profile* of the text line

$$h(y) = \sum_{x=0}^{W} f(x,y), \qquad y = t, t+1,\cdots,b$$

is the sum of grayscale along the horizontal scan-lines y. The *vertical profile* of the text line

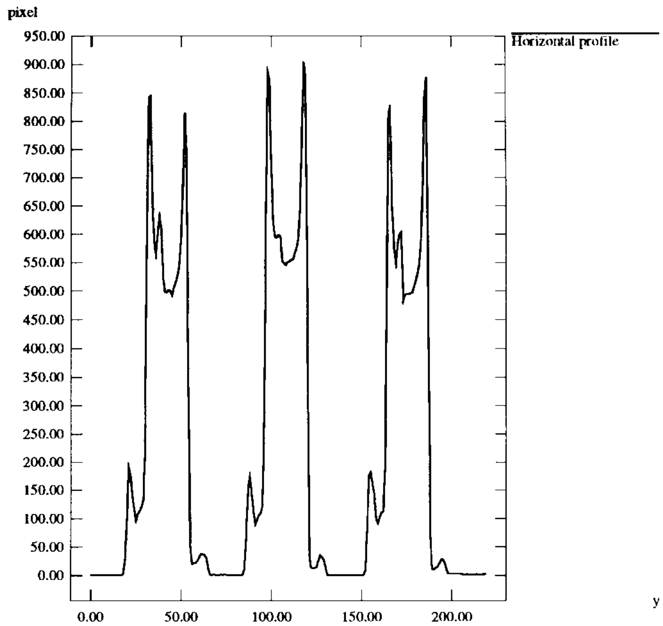
$$v(x) = \sum_{y=t}^{b} f(x,y), \qquad x = 0,1,\cdots,W$$

is the sum of grayscale along the vertical scan-lines x. For simplicity we assume that $f(x,y)$ and, hence, the profiles $h(y)$ and $v(x)$ take continuous values.

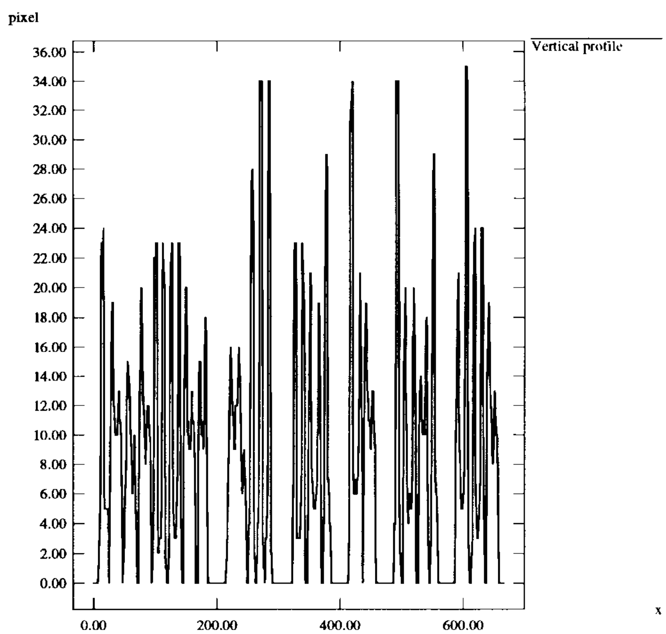
Fig. 1 shows a typical horizontal profile of three text lines and a typical vertical profile of six words. Note the different scales on the two profiles. A horizontal profile consists of distinct "columns" and "valleys." The columns correspond to text lines and the valleys correspond to interline spaces. The bulk of a column is several hundred bits for the shown digitization resolution. On the other hand, a vertical profile has shorter columns and narrower valleys that are much less distinguishable. These examples will be used later for illustration.

A text line can be marked vertically by shifting it slightly up or down from its normal position to carry one bit of the copy's unique identifier. To compensate for major distortions a line is marked only if it and its two neighboring lines are all sufficiently long. The neighboring lines, called the control lines, are not marked. Alternatively, a line can be marked horizontally by shifting certain words slightly left or right from their normal positions. The line is divided into some odd number of groups of words such that each group contains a sufficient number of characters. Each even group is then shifted while each odd group, called the control group, remains stationary. The control lines, and control groups, are used to estimate and compensate for distortions in the horizontal profile and the vertical profile, respectively.

Both line-shift and word-shift marking can be considered within the same model where we have a profile, denoted by $h(y)$, that covers three "blocks." For line-shift detection each block is the horizontal profile of a text line. For word-shift detection each block is the vertical profile of a group of words. The middle block is shifted slightly while the other two blocks, called the control blocks, are stationary.



(a)



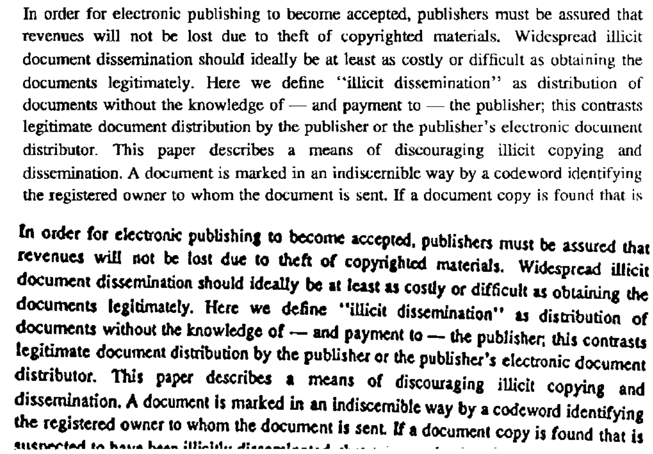
(b)

Fig. 1. (a) Horizontal and (b) vertical profile (resolution = 300 dpi).

B. Profile Noise

When the marked original is printed, photocopied, and then scanned, the text is typically distorted by translation, scaling, speckles (salt-and-pepper noise), rotation (skewing), blurring, and other random distortions. For example, a skew angle between –3° and +3° and an expansion or shrinkage of up to 2% have been observed in our experiments. From experience, photocopying introduces the most noise. A sample of an original text and its tenth copy is shown in Fig. 2.

Before document profiles are compiled, the scanned image is first processed by standard document image processing techniques [19, Ch. 4], [17], [18] to remove skewing and speckles. Then profiles are compiled from the processed image. We assume that the translation and scaling are unknown but vary slowly with respect to the distance of encoding of a bit so that they are uniform across the encoding of a bit. They are estimated using the left and right control blocks and compensated for before detection is attempted; some heuristic schemes that have been tried are given in [13].


In order for electronic publishing to become accepted, publishers must be assured that revenues will not be lost due to theft of copyrighted materials. Widespread illicit document dissemination should ideally be at least as costly or difficult as obtaining the documents legitimately. Here we define "illicit dissemination" as distribution of documents without the knowledge of — and payment to — the publisher; this contrasts legitimate document distribution by the publisher or the publisher's electronic document distributor. This paper describes a means of discouraging illicit copying and dissemination. A document is marked in an indiscernible way by a codeword identifying the registered owner to whom the document is sent. If a document copy is found that is

In order for electronic publishing to become accepted, publishers must be assured that revenues will not be lost due to theft of copyrighted materials. Widespread illicit document dissemination should ideally be at least as costly or difficult as obtaining the documents legitimately. Here we define "illicit dissemination" as distribution of documents without the knowledge of — and payment to — the publisher; this contrasts legitimate document distribution by the publisher or the publisher's electronic document distributor. This paper describes a means of discouraging illicit copying and dissemination. A document is marked in an indiscernible way by a codeword identifying the registered owner to whom the document is sent. If a document copy is found that is

Fig. 2. Sample of (top) an original text image and (bottom) its tenth copy.

This series of processing is the motivation for us to include control blocks. The major distortions affect the marked blocks and the control blocks in a similar fashion. This is exploited to remove structural distortions on the marked blocks after estimating them from the control blocks. Furthermore, by estimating the correlation structure of the remaining noise on the control blocks, the remaining noise on the marked blocks can be whitened to a significant extent.

Hence, we assume that a profile $h(y)$ on some interval $[b, e]$ after distortion compensation is corrupted only by additive noise $N(y)$ to become

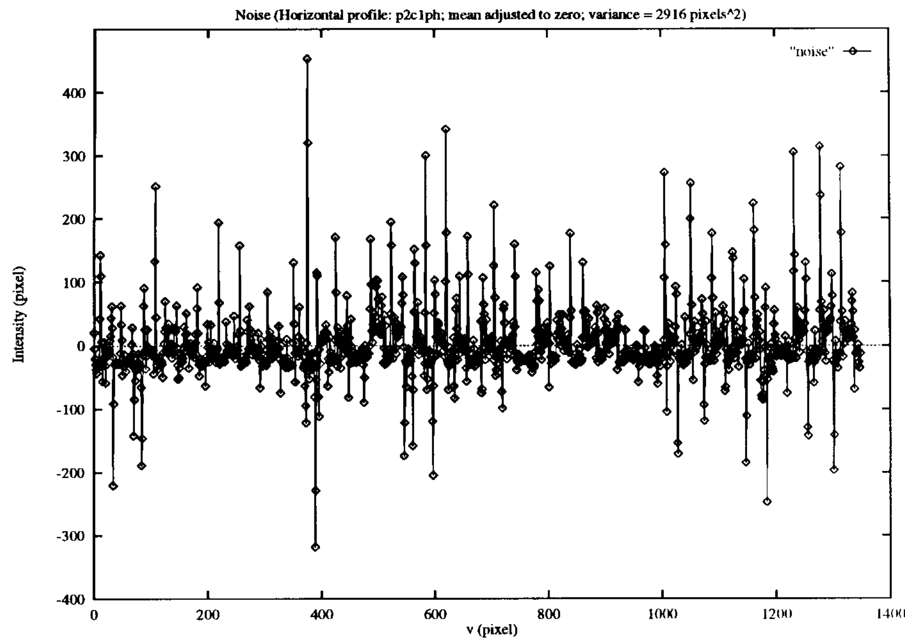
$$g(y) = h(y) + N(y), \qquad y = b, \cdots, e. \tag{1}$$

We assume that $N(y)$ are independently identically distributed (i.i.d.) Gaussian random variables with mean 0 and variance σ^2. This white Gaussian noise models all of the distortions not accounted for as well as errors introduced in the compensation. A sample of noise $N(y)$ measured from a horizontal and a vertical profile is shown in Fig. 3. The corresponding empirical distributions of $N(y)$ are shown in Fig. 4. From these figures the Gaussian model seems reasonable as a first approximation.

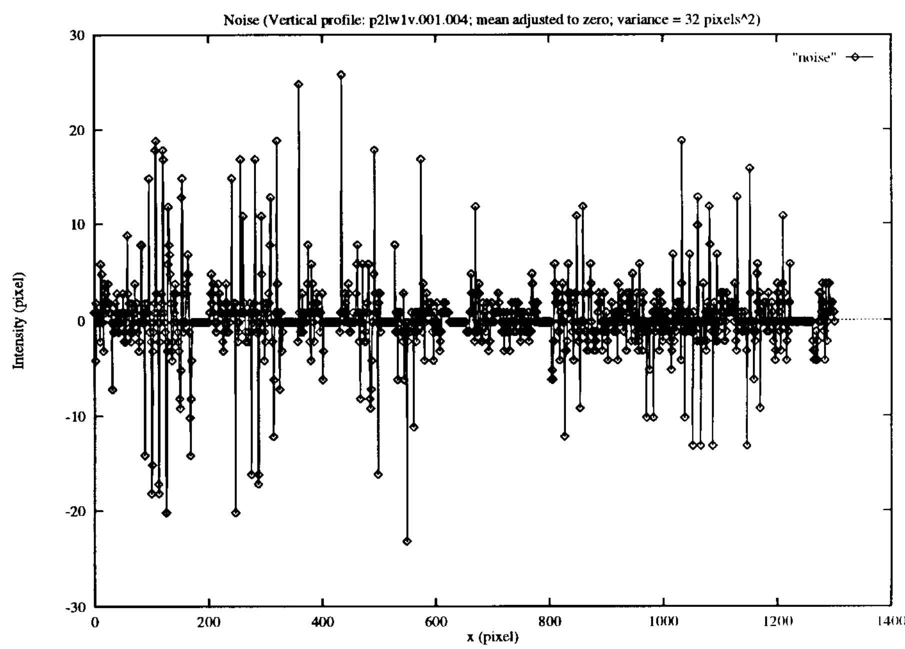
III. Centroid Noise Density

The observation that a horizontal profile consists of distinct tall and narrow columns suggests the approximation of each column by a delta function situated at the column's centroid; see Fig. 1. Marking shifts the centroid of the middle block slightly and leaves the centroids of the control blocks unchanged. The effect of translation of the entire text is eliminated by making detection decision based on the distance of the shifted centroid *relative to* its two control centroids.

In order to derive the maximum-likelihood detection, we characterize in this section the effect of additive *profile* noise on the centroid positions. The major conclusion of this section is that, for typical profiles, the centroid noise is approximately



(a)



(b)

Fig. 3. Sample profile noise measured from (a) a horizontal and (b) a vertical profile.

zero-mean Gaussian whose variance is easily computable from the original unmarked profile. This is done in three steps.

We first obtain the exact density function of the centroid noise. It depends on the structure of the original unmarked profile as well as on the variance of the additive profile noise. The exact density is, however, too complicated to be used for detection. Making use of characteristics of a typical unmarked profile, we derive a remarkably simple Gaussian approximation to the exact density. Finally we comment on the error of the approximation and illustrate the accuracy of the approximation with real document profiles.

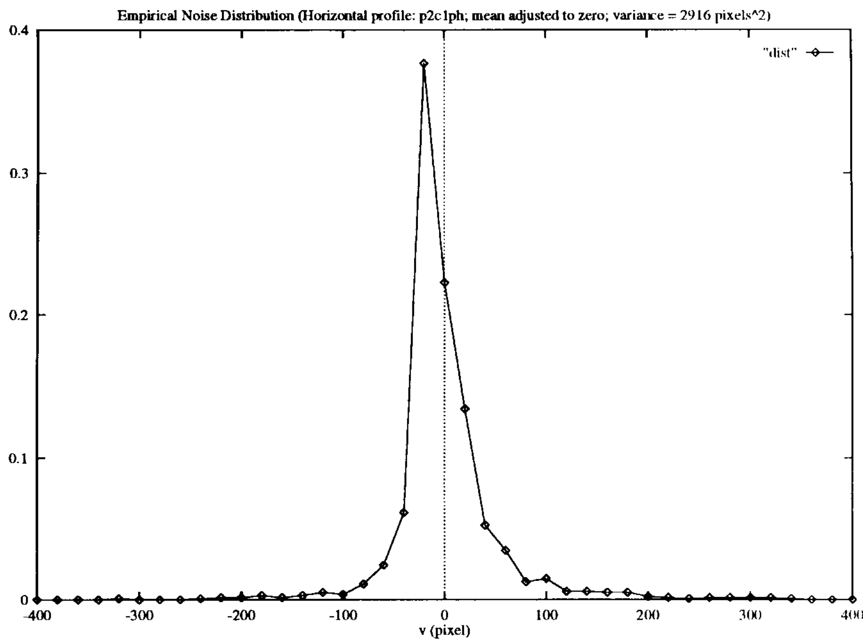
This approximation allows us to derive a maximum-likelihood detector in the next section.

A. Exact Density

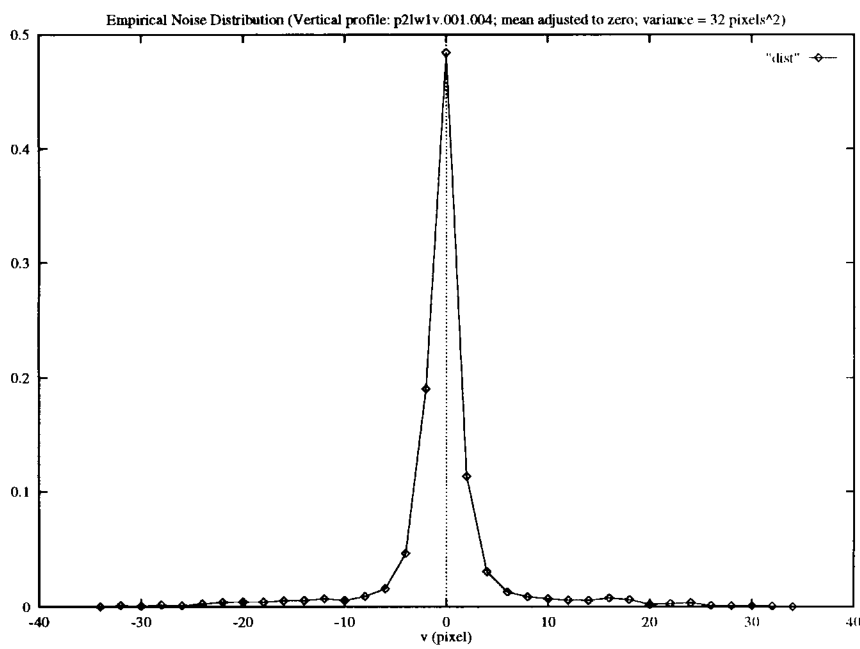
Consider a single profile block $h(y), y = b, \cdots, e$. The centroid of this uncorrupted profile $h(y)$ is defined as

$$c = \frac{\sum_{y=b}^{e} y h(y)}{\sum_{y=b}^{e} h(y)} =: \frac{M}{H}$$

where the numerator M denotes the total "moment" and the denominator H denotes the total "weight."



(a)



(b)

Fig. 4. Corresponding empirical distributions.

Suppose the profile is corrupted by white Gaussian noise $N(y)$ to become $h(y)+N(y)$ as in (1). Let its centroid be given by

$$U = c + V$$

where V is a random variable representing the distortion of the centroid by the additive Gaussian noise. We now derive the density function f_V of V.

By definition

$$\begin{aligned} V &= \frac{\sum y(h(y)+N(y))}{\sum (h(y)+N(y))} - \frac{\sum yh(y)}{\sum h(y)} \\ &= \frac{\sum \alpha(y)N(y)}{H^2 + H\sum N(y)} =: \frac{N_1}{N_2} \end{aligned}$$

where

$$\alpha(y) = yH - M. \tag{2}$$

Hence, the random variable V is the ratio of two Gaussian random variables N_1 and N_2 whose means and variances are functions of the uncorrupted profile. N_1 has zero mean and variance

$$\sigma_1^2 = \sigma^2 \sum \alpha^2(y). \tag{3}$$

N_2 has mean and variance given by

$$\mu = H^2 \qquad \sigma_2^2 = \sigma^2 H^2 (e - b + 1). \tag{4}$$

The correlation coefficient of N_1 and N_2 is

$$r = \frac{EN_1(N_2 - \mu)}{\sigma_1 \sigma_2} = \frac{\sum \alpha(y)}{\sqrt{(e-b+1)\sum \alpha^2(y)}}.$$

The joint density of (N_1, N_2) is

$$\begin{aligned} &f_{N_1,N_2}(n_1,n_2) \\ &\quad = \frac{1}{2\pi\sigma_1\sigma_2\sqrt{1-r^2}} \exp\left\{-\frac{1}{2(1-r^2)}\right. \\ &\qquad \left. \cdot \left(\frac{n_1^2}{\sigma_1^2} - 2r\frac{n_1(n_2-\mu)}{\sigma_1\sigma_2} + \frac{(n_2-\mu)^2}{\sigma_2^2}\right)\right\}. \end{aligned}$$

Being a ratio of two random variables, V has a density function given by [20, pp. 137]

$$f_V(v) = \int_{-\infty}^{\infty} |x| f_{N_1,N_2}(vx, x)\, dx.$$

Routine but tedious manipulations yield the density of the centroid noise

$$\begin{aligned} f_V(v) = &\frac{C \exp\left(-\frac{1}{2}E^2(0)\right)}{\pi A(v)} + \frac{1}{2\pi}\frac{|B(v)|}{A^{3/2}(v)} \\ &\cdot \exp\left(-\frac{1}{2}(E^2(0) - E^2(v))\right) I(|E(v)|) \end{aligned} \tag{5}$$

where

$$A(v) = \sigma_2^2 v^2 - 2r\sigma_1\sigma_2 v + \sigma_1^2 \tag{6}$$
$$B(v) = \mu(\sigma_1^2 - r\sigma_1\sigma_2 v) \tag{7}$$
$$C = \sigma_1\sigma_2\sqrt{1-r^2} \tag{8}$$
$$E(v) = \frac{B(v)}{C\sqrt{A(v)}} \tag{9}$$
$$I(v) = \int_{-v}^{v} \exp\left(-\frac{1}{2}x^2\right) dx.$$

B. Approximation Density

In this subsection, we show heuristically that the density in (5) has a remarkably simple approximation

$$f_V(v) \sim \frac{1}{\sqrt{2\pi}(\sigma_1/\mu)} \exp\left(-\frac{v^2}{2(\sigma_1/\mu)^2}\right) \tag{10}$$

i.e., V is approximately a zero-mean Gaussian random variable with variance

$$(\sigma_1/\mu)^2 = \frac{\sigma^2 w}{H^2}\left(\delta^2 + \frac{1}{12}(w^2-1)\right). \tag{11}$$

Here

$$w := e - b + 1$$

denotes the width of the profile and

$$\delta := c - \frac{e+b}{2}$$

denotes the deviation of the uncorrupted centroid from the center. Hence, the noise variance depends on the original profile $h(y)$ only through three parameters: its weight H, its width w, and the deviation δ of centroid from the center. In the next subsection we justify the approximation by exhibiting upper bounds on the error.

The variance $(\sigma_1/\mu)^2$ is typically very small for real profiles. Hence the density concentrates in the neighborhood of $v = 0$. Around $v = 0, |E(v)|$ is large. Applying the following well-known approximation:

$$\int_x^{\infty} e^{-y^2/2}\, dy \sim \frac{1}{x} e^{-x^2/2} \quad \text{for large } x$$

to $I(|E(v)|)$, we have

$$\begin{aligned} I(|E(v)|) &= \int_{-|E(v)|}^{|E(v)|} e^{-y^2/2}\, dy \\ &\sim \sqrt{2\pi} - \frac{2}{|E(v)|}\exp\left(-\frac{1}{2}E^2(v)\right). \end{aligned} \tag{12}$$

Substituting into (5) and simplifying, we obtain

$$f_V(v) \sim \frac{1}{\sqrt{2\pi}}\frac{|B(v)|}{A^{3/2}(v)} \exp\left(-\frac{1}{2}(E^2(0) - E^2(v))\right). \tag{13}$$

We approximate the scaling factor $|B(v)|/A^{3/2}(v)$ in front of the exponential term by its value at $v = 0$

$$\frac{|B(v)|}{A^{3/2}(v)} \sim \frac{\mu}{\sigma_1}. \tag{14}$$

From (6) to (9)

$$E^2(v) = E^2(0) - \frac{\mu^2 v^2}{A(v)}.$$

Using this, we approximate $E^2(v)$ in the exponent (13) by its Taylor expansion about $v = 0$

$$\begin{aligned} E^2(v) &\sim E^2(0) + \frac{d}{dv}E^2(0)v \\ &\qquad + \frac{1}{2}\frac{d^2}{dv^2}E^2(0)v^2 \end{aligned} \tag{15}$$
$$= E^2(0) - \frac{\mu^2}{\sigma_1^2}v^2. \tag{16}$$

Substituting (14) and (16) into (13) yields (10) as desired. To show (11) we have from (2)

$$\sum_{y=b}^{e} \alpha^2(y) = H^2\left(\sum_b^e y^2 - 2c\sum_b^e y + c^2 w\right)$$

where c is the uncorrupted centroid. Some algebra reduces the above expression to

$$\sum_{y=b}^{e} \alpha^2(y) = H^2 w(\delta^2 + (w^2-1)/12).$$

TABLE I
EXAMPLE PROFILE PARAMETERS

	Horizontal profile	Vertical profile
Profile noise variance σ^2	2916 pixels^2	32 pixels^2
Centroid noise variance $(\sigma_1/\mu)^2$	0.0781	2.3381
$(w^2-1)/12$	176	884
δ^2	1.31	0.024

Hence, from (3)

$$\begin{aligned}\sigma_1^2 &= \sigma^2 \sum \alpha^2(y)\\ &= \sigma^2 H^2 w(\delta^2 + (w^2-1)/12)\end{aligned}$$

yielding (11) as desired in view of (4).

Table I gives example values of some of the parameters, measured from the data in Figs. 1 and 4. We see that the deviation δ of the uncorrupted centroid from the midpoint of a profile is typically negligible. More importantly, a vertical profile typically has a larger *centroid* noise variance than a horizontal profile. This can be explained qualitatively by our approximating density: from (11), the centroid noise variance is increasing in the profile width w and decreasing in the profile weight H. Since a vertical profile block of words is wider and has much less weight (see Fig. 1) than a typical horizontal profile block, we should expect centroid noise variance to be larger for word profiles, as observed. For the effect on detection performance, see Section V-A. We remark that these parameter values, however, are sensitive to the experimental environment such as the condition of the copier and scanner, and specific document, etc.

C. Error Bounds

Let

$$g_V(v) := \frac{1}{\sqrt{2\pi}(\sigma_1/\mu)} \exp\left(-\frac{v^2}{2(\sigma_1/\mu)^2}\right)$$

be the approximating Gaussian density. By assessing the error in the Gaussian density approximation (12) and the Taylor series approximation (14), (15) we can derive upper bounds on the error $|f_V(v) - g_V(v)|$ as a function of v. In this subsection we comment on the bounds and illustrate the accuracy of the approximation with example profiles. The details are omitted due to space limitation.

There are three regions of v to consider, depending on whether both approximations are accurate, only the Gaussian density approximation is accurate, or neither approximations are accurate. In the neighborhood of $v_0 := \sigma_1/r\sigma_2$ where $B(v)$ and hence $|E(v)|$ are close to zero, the Gaussian density approximation (12) is poor. Outside this region (12) holds well. The first region to consider is around $v = 0$ ($\ll v_0$ for typical profiles) where both the Gaussian density approximation (12) and the Taylor expressions (14) and (15) are accurate. The second region is for large v where the Gaussian density approximation (12) is accurate but not the Taylor expressions (14), (15). The third region is in the neighborhood of v_0 where $|E(v)|$ is small and even the Gaussian density approximation (12) is poor.

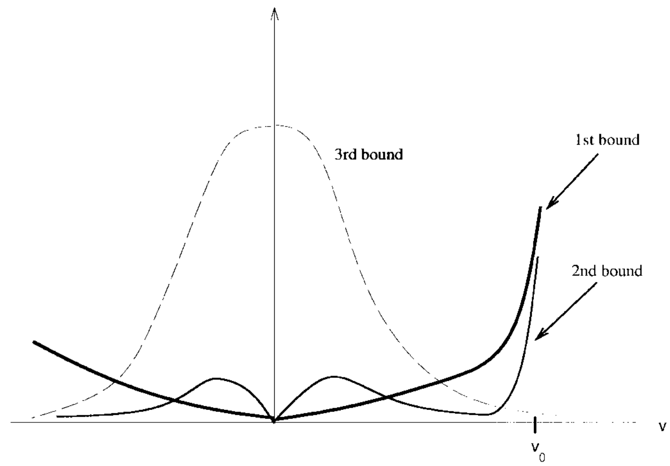


Fig. 5. Error bounds as a function of v.

We have derived a bounding function on the error $|f_V(v) - g_V(v)|$ that is composed of three separate bounding functions, one covering each region of v. The error $|f_V(v) - g_V(v)|$ lies beneath the minimum of them, as illustrated in Fig. 5. The first bound is small for v around zero. The second bound is small for $0 \ll v \ll v_0 := \sigma_1/r\sigma_2$. The third bound is small for large v near v_0 and beyond. The derivation is based on the intuition that, around $v = 0$, where the densities f_V and g_V concentrate, both approximation (12) and the Taylor expansions are accurate. Furthermore, f_V and g_V decay so rapidly that outside a small neighborhood of $v = 0$, e.g., a few multiples of the standard deviation σ_1/μ, both densities and, hence, their difference become negligible.

We now illustrate the accuracy of the approximation for typical profiles. Using $\sigma^2 = 2916$ for horizontal profile and $\sigma^2 = 32$ for vertical profile (from Table I), we compute f_V and its Gaussian approximation g_V for the second block of the horizontal profile and for the first block of the vertical profile, consisting of one word, shown in Fig. 1. The approximation is so accurate that the two curves are indistinguishable on the same plot. Instead, we plot the normalized absolute error

$$\frac{|f_V(v) - g_V(v)|}{f_V(0)}$$

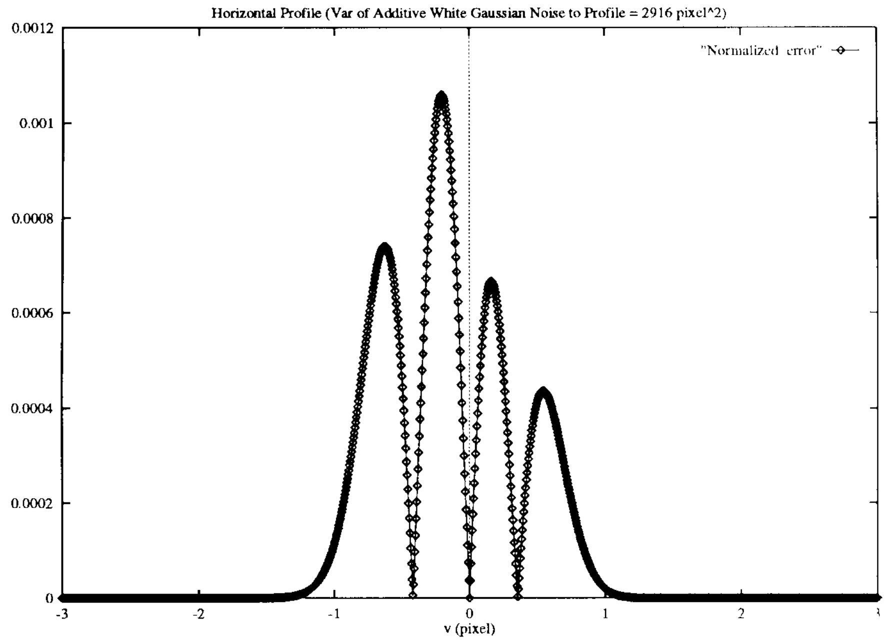
versus v in Fig. 6.

IV. CENTROID DETECTION AND PERFORMANCE

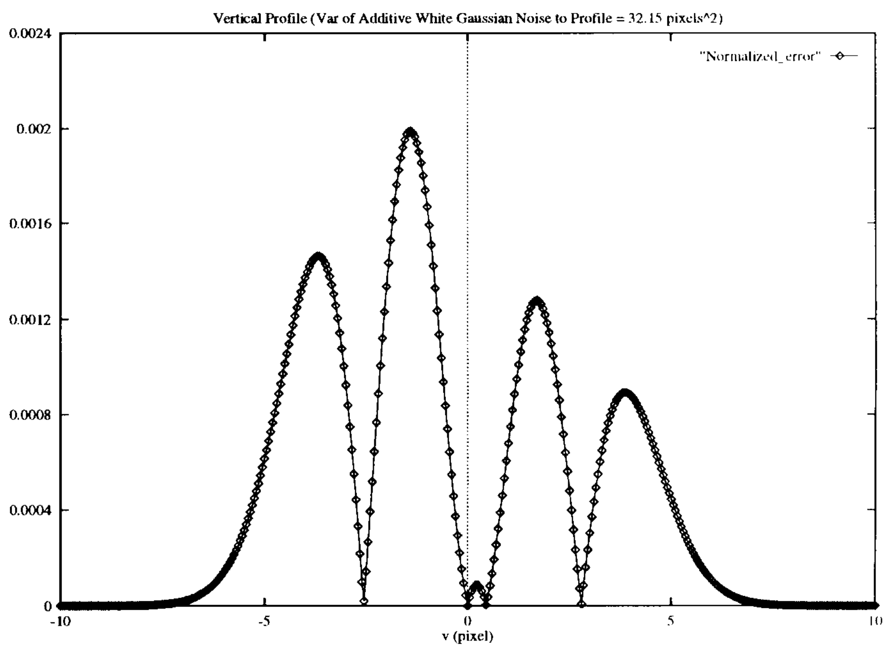
We are given an original unmarked profile $h(y)$ and its noisy marked copy $g(y)$. In this section we present a maximum-likelihood detector that uses the distances between adjacent centroids as a basis for decision.

The original unmarked profile $h(y)$ consists of three blocks defined on the intervals $[b_1, e_1]$, $[b_2, e_2]$, and $[b_3, e_3]$; see Fig. 1. The centroid of block $i, i = 1, 2, 3$ is

$$c_i = \frac{\sum_{b_i}^{e_i} y h(y)}{\sum_{b_i}^{e_i} h(y)}.$$



(a)



(b)

Fig. 6. Normalized absolute error for (a) horizontal and (b) vertical profiles.

The profile compiled from the illicit copy and after distortion compensation is

$$g(y) = h'(y) + N(y), y = b_1, b_1 + 1, \cdots, e_3$$

where $h'(y)$ is the marked but uncorrupted profile. The additive white zero-mean Gaussian noise $N(y)$ has a variance $\mathrm{var(N(y))} = \sigma^2$. The control blocks have centroids

$$U_1 = c_1 + V_1 \quad \text{and} \quad U_3 = c_3 + V_3.$$

The middle block has been shifted by a size $\epsilon > 0$ so that its centroid is

$$U_2 = c_2 + V_2 - \epsilon$$

if it is left-shifted, and

$$U_2 = c_2 + V_2 + \epsilon$$

if it is right-shifted. Since $N(y)$ is white, the centroid noise $V_i, i = 1, 2, 3$ are independent. We apply the Gaussian approximation developed in the last section to V_i. Thus, V_i is zero-mean Gaussian with variance ν_i^2 given by

$$\nu_i^2 = \frac{\sigma^2 w_i}{H_i^2}(\delta_i^2 + (w_i^2 - 1)/12) \tag{17}$$

$$H_i = \sum_{b_i}^{e_i} h(y) \tag{18}$$

$$w_i = e_i - b_i + 1 \tag{19}$$
$$\delta_i = c_i - \frac{e_i + b_i}{2}. \tag{20}$$

To eliminate the effect of translation we base our detection on the distance $U_i - U_{i-1}$ between adjacent centroids instead of the absolute position of the middle centroid U_2. We have a classical detection problem in which we have to decide whether the middle centroid has been left- or right-shifted given the observed values of $U_2 - U_1$ and $U_3 - U_2$. We next derive the maximum-likelihood detection that chooses the direction of the shift that is most likely to have caused the observed $U_2 - U_1$ and $U_3 - U_2$.

It is convenient to use as decision variables the differences

$$\Gamma_l := (U_2 - U_1) - (c_2 - c_1)$$
$$\Gamma_r := (U_3 - U_2) - (c_3 - c_2)$$

of the corrupted centroid separations and the uncorrupted separations. Γ_l is the change in the distance of the middle block from the left control block and Γ_r is that from the right control block. Without noise, $\Gamma_l = -\epsilon$ and $\Gamma_r = \epsilon$ if the middle block is left-shifted, and $\Gamma_l = \epsilon$ and $\Gamma_r = -\epsilon$ if it is right-shifted. Hence, it is reasonable to decide that the middle block is left-shifted if $\Gamma_l \le \Gamma_r$, and right-shifted otherwise. With noise, according to the following theorem, these changes in the distance of the middle block from the control blocks should be weighted by the noise variances in the centroids of the control blocks before being compared. Note that the decision does not depend on the middle block, except through Γ_l and Γ_r.

Theorem 1: The maximum-likelihood detector, when the observed value of (Γ_l, Γ_r) is (γ_l, γ_r), is

$$\begin{array}{ll} \text{decide left shift,} & \text{if } \gamma_l/\nu_1^2 \le \gamma_r/\nu_3^2 \\ \text{decide right shift,} & \text{otherwise} \end{array}$$

where ν_1^2 and ν_3^2 are the centroid noise variances of the left and right control blocks, respectively.

Note that the test in the theorem does not require measurement of the profile noise variance σ^2 since it appears in both ν_1^2 and ν_3^2 [see (17)]. Only the three parameters H_i, w_i, δ_i of each uncorrupted control block are necessary.

Proof: If the middle block is left-shifted, then

$$\Gamma_l = (V_2 - V_1) - \epsilon$$

is Gaussian with mean $-\epsilon$ and variance $\nu_1^2 + \nu_2^2$, and

$$\Gamma_r = (V_3 - V_2) + \epsilon$$

is Gaussian with mean ϵ and variance $\nu_2^2 + \nu_3^2$. Their covariance is

$$E(\Gamma_l + \epsilon)(\Gamma_r - \epsilon) = -\nu_2^2.$$

Hence, the conditional density of (Γ_l, Γ_r) given a left-shifted middle block (whose centroid is changed by $-\epsilon$) is

$$\begin{aligned} &f_{\Gamma_l,\Gamma_r|-\epsilon}(\gamma_l, \gamma_r | -\epsilon) \\ &\quad = \frac{1}{2\pi\sqrt{C}} \exp\left\{\frac{-1}{2C}(\lambda_3(\gamma_l+\epsilon)^2 + 2\nu_2^2(\gamma_l+\epsilon)(\gamma_r-\epsilon) \right. \\ &\qquad \left. +\lambda_1(\gamma_r - \epsilon)^2)\right\} \end{aligned}$$

where $\lambda_1 := \nu_1^2 + \nu_2^2, \lambda_3 := \nu_3^2 + \nu_2^2$, and $C = \lambda_1\lambda_3 - \nu_2^4 = \nu_1^2\nu_2^2 + \nu_2^2\nu_3^2 + \nu_3^2\nu_1^2$. On the other hand, if the middle block is right-shifted, then

$$\Gamma_l = (V_2 - V_1) + \epsilon, \quad \Gamma_r = (V_3 - V_2) - \epsilon$$

and the conditional density is

$$\begin{aligned} &f_{\Gamma_l,\Gamma_r|+\epsilon}(\gamma_l, \gamma_r | -\epsilon) \\ &\quad = \frac{1}{2\pi\sqrt{C}} \exp\left\{\frac{-1}{2C}(\lambda_3(\gamma_l-\epsilon)^2 + 2\nu_2^2(\gamma_l-\epsilon)(\gamma_r+\epsilon) \right. \\ &\qquad \left. +\lambda_1(\gamma_r + \epsilon)^2)\right\} \end{aligned}$$

Hence, the log-likelihood ratio is

$$\begin{aligned} R(\gamma_l, \gamma_r) &:= \log \frac{f_{\Gamma_l,\Gamma_r|-\epsilon}(\gamma_l, \gamma_r | -\epsilon)}{f_{\Gamma_l,\Gamma_r|+\epsilon}(\gamma_l, \gamma_r | \epsilon)} \\ &= \frac{2\epsilon}{C}(\nu_1^2\gamma_r - \nu_3^2\gamma_l). \end{aligned} \tag{21}$$

The maximum-likelihood decision rule chooses the direction of the shift that has the larger likelihood given the observation (γ_l, γ_r)

$$\begin{array}{ll} \text{decide left shift,} & \text{if } R(\gamma_l, \gamma_r) \ge 0 \\ \text{decide right shift,} & \text{otherwise.} \end{array}$$

Substituting (21) proves the theorem. □

We evaluate the performance of this decision rule by the average probability of error, assuming that the middle block is equally likely to have been shifted left or right *a priori*

$$\begin{aligned} P_E := \tfrac{1}{2}(&P(\text{decide left shift}|\epsilon) \\ &+ P(\text{decide right shift}| -\epsilon)) \end{aligned} \tag{22}$$

where P (decide left shift$|\epsilon$) and P (decide right shift $|-\epsilon$) are the probabilities of a wrong decision when the middle block is shifted right and left, respectively.

Theorem 2: The error probability of the maximum-likelihood detector in Theorem 1 is

$$P_E = \text{erf}\left(-\epsilon\sqrt{\frac{\nu_1^2 + \nu_3^2}{\nu_1^2\nu_3^2 + \nu_2^2(\nu_1^2 + \nu_3^2)}}\right)$$

where $\text{erf}(x) := (2\pi)^{-1/2}\int_{-\infty}^{x} e^{-y^2/2}\, dy$.

Proof: From Theorem 1

$$P(\text{decide left shift}| + \epsilon) = P(\nu_3^2\Gamma_l - \nu_1^2\Gamma_r \le 0 | + \epsilon).$$

Given a right-shifted middle block, $Z := \nu_3^2\Gamma_l - \nu_1^2\Gamma_r$ is Gaussian with mean

$$\mu_Z = (\nu_1^2 + \nu_3^2)\epsilon$$

and variance

$$\begin{aligned} \sigma_Z^2 &= \nu_3^4\text{Var}(\Gamma_l) + \nu_1^4\text{Var}(\Gamma_r) \\ &\quad - 2\nu_1^2\nu_3^2\text{Cov}(\Gamma_l\Gamma_r) \\ &= (\nu_1^2 + \nu_3^2)(\nu_1^2\nu_3^2 + \nu_2^2(\nu_1^2 + \nu_3^2)). \end{aligned}$$

The density function of Z, given a right-shifted middle block, is

$$f_{Z|\epsilon}(z|\epsilon) = \frac{1}{\sqrt{2\pi}\sigma_Z}\exp\left(-\frac{(z - \mu_Z)^2}{2\sigma_Z^2}\right).$$

Hence

$$
\begin{aligned}
&P(\text{decide left shift}|+\epsilon)\\
&\quad= \int_{-\infty}^{0} f_{Z|\epsilon}(z|\epsilon)\,dz\\
&\quad= \mathrm{erf}\left(-\epsilon\sqrt{\frac{\nu_1^2+\nu_3^2}{\nu_1^2\nu_3^2+\nu_2^2(\nu_1^2+\nu_3^2)}}\right). \qquad (23)
\end{aligned}
$$

Similar reasoning shows that P (decide left shift $|\epsilon) = P$ (decide right shift $|-\epsilon$). The claim then follows from (22) and (23). □

Remarks: The value of error probability P_E depends on the specific structure of the profile blocks through ν_i, and seems to be sensitive to the document format (width and weight of profile blocks) and to the distortions introduced in processes such as printing, photocopying, and scanning. For horizontal profiles, however, it is common that adjacent text lines, being close together, have similar length and density and suffer a similar amount of distortion. In this case, ν_i are roughly equal for $i = 1, 2, 3$. Then the error probability $P_E = \mathrm{erf}(-\epsilon\sqrt{2/3\nu_1^2})$. Using the value for $\nu_1^2 = 0.0781$ from Table I for horizontal profiles and a shift size of $\epsilon = 2$ pixels, $P_E = 2.56 \times 10^{-9}$. Though it is difficult to verify such a small probability experimentally, the prediction seems consistent with the very reliable detection we have experienced in experiments [3], [11].

The current model seems also useful to explain *qualitatively* many of our empirical observations. For instance, we observed empirically in [3] that the *centroid* noise can be well approximated by Gaussian distribution. This observation can be justified theoretically by the derivation in the last section. For another instance, the experimental result that centroid detection performs much better on line shifts than on word shifts can be explained by the analytical results in the last section and this section; see Section V-A and [12]. Using the value for $\nu_1^2 = 2.3381$ from Table I for vertical profiles and a shift size of $\epsilon = 2$ pixels, $P_E = 0.143$, a much larger error probability than that predicted for line shifting.

V. Experimental Results and Prototype

In this section we present two sets of experimental results of centroid detection, one for line shifts quoted from [11] and the other for word shifts quoted from [4]. Then we describe a document marking and detection prototype that has implemented the proposed algorithm.

A. Experimental Results

In the first experiment a two-page document, the first page being a title page, were marked by line shifting. They were printed on a Hewlett–Packard LaserJet IIISi laser printer. Recursive copies were made on a Xerox 5052 plain paper copier to create successively more degraded copies. The copies were scanned using a Ricoh FS2 Apunix scanner to produce bitmap images. These images were processed to generate vertical and horizontal profiles. Marking was detected from these profiles using centroid detection.

Page 1 of the document contained eight marked lines and page 2 contained 11, giving a total of 19 marked lines. Each of these lines was shifted vertically by 2 pixels, or 1/150 in. Denote the laser printed copy as copy 0; the ith copy $i = 1, \cdots, 10$ is obtained by photocopying copy $i-1$. The detection result is shown in Table II. The perfect result was a bit surprising given the severe distortion to the photocopies; see Fig. 2.

TABLE II
Centroid Detection of Line Shifts (Shift = 1/150 In)

Copy	Error Rate
0 - 10	0/19

TABLE III
Centroid Detection of Word Shifts (Shift = 1/150 in)

Copy	Error Rate
0	3/177
3	32/177
4	43/177

We have also transmitted copy 0 by facsimile and applied centroid detection on the received copy. All 19 line shifts were correctly detected. An interesting method is proposed in [15] to watermark a facsimile image by perturbing the run-lengths of successive 1's (black pixels) in the image. There are several differences in their method and ours, stemming from the fact that theirs is a general image-marking technique whereas ours is restricted to formatted text documents. Their method can generally embed more bits than ours since there are many more clusters of black pixels than lines or words on a page. However, we expect that their method is not as robust as ours against distortions introduced by printing, photocopying, and scanning (detection in the presence of noise is not presented in [15] nor is any experimental result). In their method, each cluster of black pixels is perturbed independently. In contrast, shifting a line in our method perturbs many clusters of black pixels simultaneously, increasing the "signal strength," and centroid detection exploits these correlated movements in detecting the marks in the presence of noise.

In the second experiment a single-page document was marked by word shifting. The test page contained 177 words that were shifted horizontally by 2 pixels, or 1/150 in. It was printed and recursively photocopied four times. These copies were scanned, the bitmap images were processed, vertical profiles of words were compiled, and the word shifts were detected using centroid detection. The detection result is shown in Table III.

From the two experiments we observe that centroid detection of word shifts is much worse than that of line shifts. This confirms the theoretical prediction of Sections III and IV.

B. Prototype

An experiment in [13] reveals that depending on what type of processes a document goes through, the noise on the profiles after distortion compensation can be much more severe in one direction than in the other. For example, when a document is photocopied, depending on the copier and the copying option selected, the distortion can be more severe in the horizontal direction of the text. To take advantage of this possibility we propose in [13] a marking and identification strategy in which a line is marked both vertically, using line shift, and horizontally, using word shift. To detect the marking, the probability of detection error on horizontal and vertical profiles are estimated after common distortions have been compensated for. Detection is then made in the less noisy direction. This strategy has been implemented in a software prototype.

The marking subsystem takes as input the postscript file of a document and a list of its intended recipients. Each recipient is assigned a unique binary identifier. It marks a line vertically by shifting it slightly, e.g., 1/150 in, up or down from its normal position. The same line is also divided into some odd number of groups of words. Each even group is then shifted slightly, e.g., 1/150 in, left or right while the odd groups remain stationary. Instead of using multiple groups to carry multiple bits per line, we use them to carry just one bit with redundancy to combat noise. The system automatically marks the document, stores the identifier with the corresponding recipient in a database, and either generates a bitmap or prints a hard copy for each recipient.

When an illicit copy is discovered, a marked page is scanned and processed. Both horizontal and vertical profiles are compiled. The prototype then detects line shifts or word shifts accordingly as the horizontal or vertical profile is less noisy. In view of the experimental and analytical results presented here, we have implemented the centroid detector in the prototype for line shifts, and a different detection algorithm described in [12] for word shifts.

VI. Concluding Remarks

A way to discourage illicit redistribution of documents is to mark each document copy so that the original recipient can be identified from an illicit copy. Exploiting the regular structure of a text document, we embed a unique and indiscernible mark in the text by shifting certain lines slightly up or down or certain words slightly left or right from their normal positions. In this paper we have developed an algorithm to detect such minute shifts based on the movement of line or word centroids.

Centroid detection has performed remarkably well for line shifts in the presence of noise introduced by common processes a document might be subjected to, such as printing, photocopying, scanning, and facsimile transmission. Analytical and experimental results, however, indicate that centroid detection will perform poorly on word shifts. This has motivated a different detection method for word shifts, reported in [12].

This algorithm has been implemented in a document marking and identification system and preliminary experimental results have been presented.

References

[1] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," in *Proc. SPIE*, Feb. 1991, pp. 2420–2440.

[2] D. Boneh and J. Shaw, "Collusion secure fingerprinting for digital data," Comput. Sci. Dep., Princeton Univ., Princeton, NJ, Tech. Rep. CS-TR-468-94, 1994.

[3] J. Brassil, S. Low,. N. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," *IEEE J. Select. Areas Commun.*, vol. 13, pp. 1495–1504, Oct. 1995.

[4] ——, "Hiding information in document images," in *Proc. 1995 Conf. Information Sciences and Systems*, Baltimore, MD, Mar. 1995, pp. 482–489.

[5] G. Caronni, "Assuring ownership rights for digital images," in *Proc. Reliable IT Systems, VIS'95*, 1995.

[6] A. K. Choudhury, N. F. Maxemchuk, S. Paul, and H. Schulzrinne, "Copyright protection for electronic publishing over computer networks," *IEEE Network*, vol. 9, pp. 12–21, May/June 1995.

[7] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," in *Proc. First Int. Workshop Information Hiding*, Ross Anderson, Ed. Cambridge, U.K.: Springer-Verlag, May/June 1996, pp. 183–206.

[8] Special Issue on Copyright and Privacy Protection, *IEEE J. Select. Areas Commun.*, vol. 16, to be published.

[9] E. Koch, J. Rindfrey, and J. Zhao, "Copyright protection for multimedia data," in *Proc. Int. Conf. Digital Media and Electronic Publishing*, 1994.

[10] E. Koch and Z. Zhao, "Toward robust and hidden image copyright labeling," *Proc. 1995 IEEE Workshop on Nonlinear Signal and Image Processing*, June 1995.

[11] S. H. Low, A. M. Lapone, and N. F. Maxemchuk, "Document identification to discourage illicit copying," in *Proc. GLOBECOM'95*, Singapore, Nov. 1995, pp. 1203–1208.

[12] S. H. Low and N. F. Maxemchuk, "Performance comparison of two text marking and detection methods," *IEEE J. Select. Areas Commun.*, to be published.

[13] S. H. Low, N. F. Maxemchuk, J. T. Brassil, and L. O'Gorman, "Document marking an didentification using both line and word shifting," in *Proc. Infocom'95*, Boston, MA, Apr. 1995, pp. 853–860.

[14] B. M. Macq and J.-J. Quisquater, "Cryptology for digital TV broadcasting," *Proc. IEEE*, vol. 83, pp. 944–957, 1995.

[15] K. Matsui and K. Tanaka, "Video-steganography," in *IMA Intellectual Property Project Proc.*, vol. 1, 1994, pp. 187–206.

[16] N. F. Maxemchuk and S. H. Low, "Marking text documents," in *Proc. Int. Conf. Image Processing*, Santa Barbara, CA, Oct. 1997.

[17] L. O'Gorman, "Image and document processing techniques for the RightPages electronic library system," *Int. Conf. Pattern Recognition (ICPR)*, Sept. 1992, pp. 260–263.

[18] ——, "The document spectrum for structural page layout analysis," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 15, pp. 1162–1173, Nov. 1993.

[19] L. O'Gorman and R. Kasturi, "Document image analysis," in *IEEE Computer Society Tutorial Text Series*. New York: IEEE Press, 1994.

[20] A. Papoulos, *Probability, Random Variables, and Stochastic Processes*, 2nd ed. New York: Mc-Graw Hill, 1984.

[21] J. O. Ruanaidh, W. J. Dowling, and F. M. Boland, "Phase watermarking of digital images," in *Proc. IEEE ICIP96*, Lausanne, Switzerland, 1996, pp. 239–242.

[22] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Transparent robust image watermarking," in *Proc. IEEE ICIP96*, Lausanne, Switzerland, 1996, pp. 211–214.

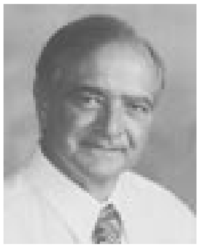
[23] K. Tanaka, Y. Nakamura, and K. Matsui, "Embedding secret information into a dithered multi-level image," in *Proc. 1990 IEEE Military Communications Conf.*, Sept. 1990, pp. 216–220.

[24] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Int. Conf. Image Processing*, vol. 2, Austin, TX, 1994, pp. 86–90.

Steven H. Low (S'88–M'92) received the B.S. degree from Cornell University, Ithaca, NY, in 1987, and the Ph.D. degree from the University of California, Berkeley, in 1992, both in electrical engineering.

He was a Consultant to NEC in the U.S. in 1991 and was with AT&T Bell Laboratories from 1992 to 1996. In 1996 He joined the University of Melbourne, Australia, as a Senior Lecturer. He has held visiting academic positions in the U.S. and Hong Kong, and has consulted with companies in Australia and the U.S. His research interests are in the control and optimization of communications networks and protocols, and network security and privacy.

Dr. Low is a co-recipient of the 1997 IEEE William R. Bennett Prize Paper Award and the 1996 R&D 100 Award. He is on the editorial board of the IEEE/ACM Transactions on Networking. He was on the Program Committee of the Workshop on Information Hiding held at the Newton Institute for Mathematical Science, University of Cambridge, in 1996.



Nicholas F. Maxemchuk (M'72–SM'85–F'89) received the B.S.E.E. degree from the City College of New York, NY, and the M.S.E.E. and Ph.D. degrees from the University of Pennsylvania, Philadelphia.

He is currently a Technical Leader with AT&T Laboratories, Florham Park, NJ. From 1976 to 1996 he was with AT&T Bell Laboratories, first as a member of the Technical Staff and then as a Department Head, and from 1968 to 1976 he was a member of the Technical Staff at the RCA David Sarnoff Research Center, Princeton, NJ. He has been on the adjunct faculties of Columbia University and the University of Pennsylvania. He has been an Advisor on data networking to the United Nations, the National Science Foundation, the Rome Air Development Center, the Canadian Institute for Telecommunications Research, the Information Technology Research Center, the Telecommunications Research Institute of Ontario, and other organizations.

Dr. Maxemchuk has served as the Editor for Data Communications for the IEEE TRANSACTIONS ON COMMUNICATIONS and as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (J-SAC). He is currently on J-SAC's Editorial Board and on the steering committee of the IEEE/ACM TRANSACTIONS ON NETWORKING. He was awarded the RCA Laboratories Outstanding Achievement Award in 1970, the Bell Laboratories Distinguished Technical Staff Award in 1984, the IEEE's Leonard G. Abraham Prize Paper Award in 1985 and 1987, and the William R. Bennett Prize Paper Award in 1997. He also received the 1996 R&D 100 Award for his work on document marking.

Aleta M. Lapone received the B.S. degree in mathematics and computer science from Montclair State College, Montclair, NJ, in 1979, and the M.S. degree in computer science from Rutgers University, New Brunswick, NJ, in 1982.

Since 1979 she has been with Bell Laboratories, Murray Hill, NJ, where she is a member of the Technical Staff. Her current interests are in software systems, the World Wide Web, Internet services, and digital libraries. She is currently managing the Bell Labs web site (www.bell-labs.com).