On the Security of Copy Detectable Images

Justin Picard; ATT Advanced Track & Trace; Rueil-Malmaison, France; j.picard@att-fr.com

Abstract

Digital watermarks, sparse dot patterns, and copy detection patterns are different types of copy-detectable images that have been used to protect documents and other physical objects against counterfeiting. There is a frequent claim about these technologies that they are "virtually impossible to copy" or "extremely hard to forge". But can this claim be quantified? This paper investigates this question from a detection theoretic viewpoint, and shows that under certain conditions, a copy falsely detected as an original is extremely improbable.

Introduction

Digital watermarks [1, 5], sparse dot patterns [2], and copy detection patterns [3] are different types of digital images that have been used to protect documents and other physical objects against copying. Combined to variable data printing, these copy detectable images (CDI), printed with standard ink and paper, become a kind of 2D barcode with enhanced security, an "all-in-one" security element that enables both identification and authentication, at an extremely low material and integration cost.

CDIs are different implementations of the same underlying principle, that printing is a noisy process through which a copy must go twice. Therefore, a carefully designed signal or image will be additionally damaged during a copy attempt: by measuring the level of degradation, a detector can tell whether a given document is an original or not. Data encryption of the CDI protects the logical layer, while the sensitivity of the signal to copy protects the physical layer.

There is a frequent claim about these technologies that they are "virtually impossible to copy", "extremely hard to forge", etc. But what does that mean exactly? Of course, they resist casual photocopying, but would they resist to a gang of determined counterfeiters ,with acute image processing skills, equipped with high resolution scanners and high end printing equipment? Are these graphics *provably* impossible to copy, at least in theory?

This paper intends to investigate this question from a decision theoretic viewpoint, noting that practicalities of using CDIs, which may significantly affect their performance [4], are not dealt with in this paper. First, we analyze the sequence of steps to produce a good copy, which we call the "copy channel", and conclude on the desirable properties of copy detectable codes. Then, we formulate the problem in a detection theoretic framework, and derive results to quantify the performance of the CDIs.

The copy channel

Clearly, there are two steps in the channel when an original is printed: (1) printing the source image and (2) digitizing for detection (here we do not consider wearing). When it is a copy, different channels are possible, whether it is a photocopy, a copy made by a purely analog mean, etc. However, we consider here the case of skilled counterfeiters, who will use digital means to maximize their chance of making an undetectable copy. In that case, the typical channel includes (1) printing the source image, (2) digitizing to prepare for a copy, (3) processing the digitized image, (4) printing the copy, and (5) digitizing for detection.

In order for a copy to be discernable from an original, there must be some modifications or degradations occurring to the CDI during steps 2 to 4. Let us examine these steps:

- Digitizing: unfortunately, the safe assumption is that the counterfeiter will use a high resolution and virtually noiseless scan, to produce his copy. In principle, twice the printing resolution would suffice, which is trivial to reach: low cost image processing are capable of 10000dpi and more (eventually with a small capture window, but multiples images can be combined). One cannot hope for any image degradation during this step.
- Processing: in this step, the counterfeiter must prepare the digitized image for printing in a compatible format. First, the counterfeiter will reconstruct all elements having a recognizable structure, colour, or semantics, such as fonts, barcode and 2D barcode elements, CMYK or pantone colour, etc. It is safe to assume that all image elements with a "meaning" (i.e. not purely random for a human) will be restored to their exact original value.
  The counterfeiter cannot take the same approach with the CDI because it is composed of elements with random values. Of course, there must be ambiguity in the determination, which can be achieved with elements taking random values that are sufficiently close so that they cannot be reliably distinguished. For instance, sparse dot patterns should have dots that are so small that they cannot be reliably discerned from the background (this is hard to achieve reliably in practice). We note that the fact that the pattern is invisible to the naked eye is not sufficient: if it can be revealed by a high resolution scan, with some simple processing it will be totally reconstructed. As we will see below, the CDI must actually take values that are "hidden", to some extent, by the printing noise.
- Copy printing: Often, counterfeits are of inferior print quality because the counterfeiter wishes to minimize its costs. However, here it is a safe assumption that the counterfeiter is willing, if necessary, to accept a cost of producing a copy that is roughly similar to the cost of producing an original print, in order to have a similar printing quality between original and copies. Therefore, the level of noise during printing should be roughly equivalent for original prints and copies.

Let us summarize our findings: (1) the source CDI image must be non-predictable from its printed version, and a precondition is that the relevant elements are generated pseudo-randomly, for instance using a secret key and a message.(2)

the values of the CDI elements should be adjusted to the printing noise level, to be "hidden" such that they cannot be non-ambiguously determined from a high resolution scan. However, we note that the noise should not be excessive, because if the CDI elements are too significantly damaged in the source printing, an insignificant amount of information would remain to be degraded during the printing of the copy, and the CDI would simply be unreadable. Between insufficient and excessive noise, there should be an optimal value: what is it? Next section proposes a mathematical model to answer this question.

A decision-theoretic model of copy detection

This section takes a detection-theoretic view point to the problem of discerning copies from originals. In our model, it is assumed that the CDI elements possess two possible values. This assumption may sound restrictive, but it actually fits well the discrete nature of most printers, which process binary images. Furthermore, sparse dot patterns, copy detection patterns and digital watermarks are usually found in binary form (for the latter, a binary message is modulated). The printing of the graphic is modeled by additive Gaussian noise. Following the preceding discussion, it is also assumed that a copy is modeled as Gaussian noise with the same energy level.

The copy is made by a "perfect" scanning of one original. In variable printing, only one print of a source CDI should exist. Using each print to produce only one copy would also greatly increase the counterfeiter's effort, who would have to collect multiple originals, and repeat the digitizing and processing steps for each of them. During the processing step, the counterfeiter cannot reproduce the real values he observes in the scan of an original print, because halftoning would binarize the image anyway. He therefore has to make a guess that will minimize his error on the source CDI value.

We denote s as the source signal, n and n_c as the printing noise for the original resp. the copy, and x as the received signal. All signals are vectors of size N.

Without loss of generality, the source signal, derived from a key and message, is binary equiprobable, i.e. $s[i] \sim \{+a, -a\}$, for $i = 0, 1, ..., N-1$, and $a > 0$. The printing noise is distributed according to $N(0, \sigma^2)$ for both original and copies, where σ is the noise energy level.

The counterfeiter receives $x = s + n$, and is constrained to process it to obtain a binary signal equal to one of $\{+a, -a\}$. Obviously, to minimize his estimation error, the counterfeiter will restore the signal value to the closest of $+a, -a$. Therefore, the detection problem is to distinguish between the two hypotheses:

$$H_0: \quad x[i] = s[i] + n[i] \qquad (1)$$

$$H_1: \quad x[i] = a.sign(s[i] + n[i]) + n_c[i] \qquad (2)$$

where H_0 and H_1 are the hypotheses that the received signal is an original, resp. a copy.

Let us now derive the optimal detector, and from the detector statistics, the optimal signal to noise ratio between the CDI values and the printing noise.

We note that the probability that the counterfeiter has correctly estimated the source signal is: $p(a.sign(s[i] + n[i]) = s[i]) = Q(-a/\sigma)$, where $Q(x) = (2\pi)^{-1/2} \int_{-a/\sigma}^{+\infty} \exp^{-x^2/2} dx$.

We have the following probability distributions for the received signals. For H_1 we have a mixture of two Gaussian distributions corresponding to the correct and incorrect guesses:

$$p(x; H_0) = \frac{1}{(2\pi\sigma^2)^{N/2}} \exp[-\frac{1}{2\sigma^2} \sum_{i=0}^{N-1} (x[i] - s[i])^2] \quad (3)$$

$$p(x; H_1) = \frac{1 - Q(-a/\sigma)}{(2\pi\sigma^2)^{n/2}} \exp[-\frac{1}{2\sigma^2} \sum_{i=0}^{N-1} (x[i] + s[i])^2] \quad (4)$$

$$+ \frac{Q(-a/\sigma)}{(2\pi\sigma^2)^{n/2}} \exp[-\frac{1}{2\sigma^2} \sum_{i=0}^{N-1} (x[i] - s[i])^2] \quad (5)$$

the Neyman-Pearson detector decides H_0 if the log likelihood ratio exceeds a threshold t:

$$\log L(\mathbf{x}) = \log \frac{p(\mathbf{x}; H_0)}{p(\mathbf{x}; H_1)} > t \qquad (6)$$

Replacing the probability distributions leads to the following simple correlator function $T(x, s)$, which must exceed a predetermined threshold t:

$$T(x, s) = \sum_{i=0}^{N-1} x[i]s[i] > t \qquad (7)$$

The optimal classification function is therefore a simple correlator.

To determine the detector statistics, we may assume that $T'(x, s)$ follows a Gaussian distribution, which is true for large N, and we can derive its expected value and variance for the two hypotheses:

$$E[T'; H_0] = Na^2 \qquad (8)$$

$$E[T'; H_1] = (2Q(-a/\sigma) - 1)Na^2 \qquad (9)$$

$$Var[T'; H_0] = Na^2\sigma^2 \qquad (10)$$

$$Var[T'; H_1] = Na^2\sigma^2 + \qquad (11)$$

$$Na^4 Q(-a/\sigma)(1 - Q(-a/\sigma))) \qquad (12)$$

The second term in the variance of T' for hypothesis H_1 ($Na^4 Q(-a/\sigma)(1 - Q(-a/\sigma))$) is caused by the variance in the estimation of s by $a.sign(s + n)$. This term applies only if each copy would be generated from a different original, which is in contradiction with our assumption that all copies come from one original. For this reason, we eliminate this term, in which case we obtain that $Var[T'; H_0] = Var[T'; H_1]$. Of course, this facilitates the statistical analysis, because in the case of equal variance, detection performance is fully characterized by the deflection coefficient d^2:

$$d^2 = \frac{(E[T'; H_0] - E[T'; H_1])^2}{Var[T'; H_0]} \qquad (13)$$

$$= 2N(\gamma(1 - Q(\gamma)))^2 \qquad (14)$$

where $\gamma = a/\sigma$. Our objective is to maximize detection performance, which is equivalent to maximizing $(\gamma(1 - Q(\gamma)))^2$.

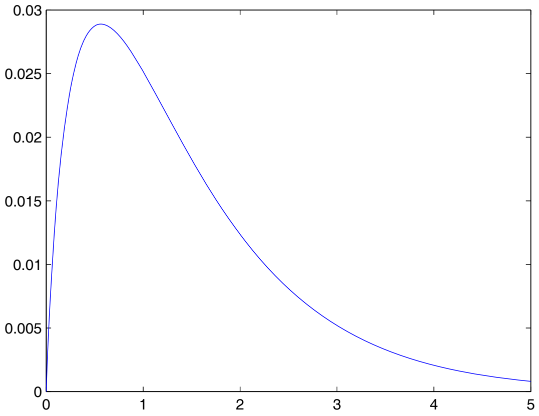

Figure 1. *Detection performance versus SNR.*

Considering that $snr = a^2/\sigma^2$ is the Signal to Noise Ratio, it is interesting to examine the function $snr.(1-Q(\sqrt{snr}))^2$. A plot of this function is represented in Figure 1. For low snr, the signal is too noisy and detection is penalized. At high snr, the source signal is of too high quality, and in most cases is correctly reconstructed. Between th two extremes, there is an optimum, for which we have not found an analytical estimate. However, a reasonable numerical estimate is: $snr \simeq 0.562$. We note that for this SNR value, the probability of error in estimating the source signal for the counterfeiter is: $p \simeq 0.226$.

A CDI optimally designed for $snr = \gamma^2 = 0.562$, having 2000 elements (most CDIs have significantly more elements), would have a deflection ratio of 114.84. For this value, the equal error rate is: 4.210^{-8}.

Conclusion

In this paper, we have investigated the problem of designing codes that allow copy detection of documents. Provided certain assumptions, we have found the optimal SNR for binary codes, which are representative of most situations. For this optimal SNR, extremely high detection performance is found.

Practicalities of using CDI, which may significantly affect their performance, were not dealt with in this paper. In future work, we will explore the impact of integrating practical aspects in the proposed theoretical model, for instance by considering an imperfect image capture when reading the CDI, and other hypotheses on the distribution of printing noise.

References

[1] H.L. Brunk, Halftone watermarking and related applications, US patent 6694041

[2] M. Jordan, F. Kutter and N. Rudaz, Method to apply an invisible mark on a media, WO2006087351

[3] J. Picard, Digital authentication with copy-detection patterns, Optical Security and Counterfeit Deterrence Techniques V, 2004

[4] J. Picard, Copy Detectable Images: From Theory to Practice, Optical Document Security, 2008.

[5] G. Rhoads and A. Gustafson, Multiple watermarking techniques for documents and other data, US patent 6332031

Author Biography

Justin Picard received his BS in physics and Master in electronics from Ecole Polytechnique de Montreal (1994), and his PhD in computer science from the University of Neuchatel, Switzerland (2000). He was a research assistant at EPFL, Switzerland, until 2001. From 2001 to 2004, he was a R&D engineer at Mediasec Technologies LLC in Providence, USA. In 2004, he became head of research at Thomson content security division in Germany. From 2006 to 2008, he was consultant in media and document security in Switzerland. He is now director of research at Advanced Track & Trace in France, where he is working on new solutions for anti-counterfeting applications of products and documents. .