Forensic Authentication of Data Bearing Halftones

Stephen Pollard[1], Robert Ulichney[2], Matthew Gaubatz[3] and [4]Steven Simske
[1]*Hewlett Packard Labs, Bristol, U.K.*
[2]*Hewlett Packard Labs, Andover, Massachusetts, U.S.A.*
[3]*Hewlett Packard Labs, Bellevue, Washington, U.S.A.*
[4]*Hewlett Packard Labs, Fort Collins, Colorado, U.S.A.*

Keywords: Forensic Printing, Stegatones, Image Registration, Gabor Filters, Biometrics.

Abstract: This paper introduces a practical system for combining overt, covert and forensic information in a single, small printed feature. The overt "carrier" feature need not be a dedicated security mark such as a 2D or color barcode, but can instead be integrated into a desirable object such as a logo as part of the aesthetically-desired layout using steganographic halftones (Stegatones). High-resolution imaging in combination with highly accurate and robust image registration is used to recover, simultaneously, a unique identity suitable for associating a unique print with an on-line database and a unique forensic signature that is both tamper and copy sensitive.

1 INTRODUCTION

Counterfeiting, warranty fraud, product tampering, smuggling, product diversion and other forms of organized deception are driving the need for improved brand protection. The potential for security printing and imaging to provide an extremely cost-effective forensic level of authentication is well-recognized (Pizzanelli, 2009). There are also a number of instances in which embedding data in hard copy is desired, but overt marks such as bar codes would damage the aesthetics of the document. The novel method, outlined in this paper, simultaneously addresses both of these needs by combining forensics and steganographic halftoning (Ulichney et al., 2010) on the same printed object, and describes a system for both encoding and decoding such objects.

In order to perform a forensic authentication of printed material, it is necessary use an image resolution sufficient to expose unique properties of the print that are extremely difficult, if not impossible on a regular paper substrate, to reproduce or copy (Pollard et al., 2010). For the majority of printing technologies, these properties result naturally from the stochastic nature of the print process itself and its interaction with the underlying structural properties of the substrate material on which ink is printed. As such they represent a unique fingerprint that can be used to authenticate individually printed items such as labels, documents, product packaging and monetary notes.

Previously (Pollard et al., 2012) a method derived from iris recognition (Daugman, 1993) has been used to derive a general area-based print signature that can be applied to halftones images and thus affords general utility and applicability for forensic print authentication. Here that idea is extended to show that the methodology developed for regular halftones is applicable to steganographic halftone, or Stegatone, images where the content of the original halftone has been modulated, in a manner unknown to the decoding system, to carry extra covert information. Most importantly, the image alignment strategy on which the method is founded is not disrupted by the introduction of unknown deformations in the printed material. Furthermore, despite the small extent of the stegatones used in our experiments (4mm on a side), they are able to encode sufficient bit data to be a practical alternative overt 2D barcode alternatives such as Data Matrix or QR-Codes.

2 METHOD

The Stegatone encoding system outlined in Figure 1 allows the creation of a secure hardcopy document with an embedded payload along with the filing of its forensic signature in a registry located on a

Pollard S., Ulichney R., Gaubatz M. and Simske S..
Forensic Authentication of Data Bearing Halftones.
DOI: 10.5220/0004296201090113
In *Proceedings of the International Conference on Computer Vision Theory and Applications* (VISAPP-2013), pages 109-113
ISBN: 978-989-8565-48-8

server. The selected target (or mule) image when printed (e.g. automatically inserted in the top right hand corner of every page during the print process) is modified to include payload information that is able to uniquely identify the document and – either directly or referentially (through the registry) – identify the user, time and location of the print.

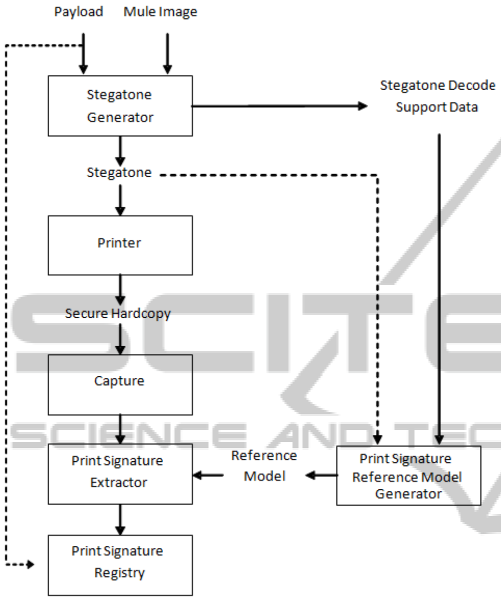


Figure 1: Forensic Stegatone encoding system.

2.1 Stegatone Generation

A Stegatone generator takes a data payload and an input image called a "mule" because it is the vehicle that transports the payload when printed. In this paper, we are using a 4mm square grayscale image as the mule to carry the payload. This image can represent any type of object including, glyphs, logos or natural images (though at this scale the content of a natural image is somewhat limited). Two example 92x92 pixel (4mm square at 600dpi) continuous tone mule images are shown at many times their actual size in Figure 2.

Reference halftones (e.g. Figure 3(a)) are standard clustered-dot halftones generated from the mule image. All halftone cells are classified in a reference map as either 0-bit, 1-bit, 2-bit, or 3-bit data carriers. These cells are depicted in Figure 3(b). 0-bit carriers, colored black, are called "Reference Cells" because they are unchanged and can be used to aid alignment. The red, green and blue cells represent 1, 2 & 3-bit carriers respectively (as they can shift in one of 2, 4 and 8 positions). Cells can be reference cells because they are too large to be shifted or too small to be detected; but, more interestingly, we can force cells to be reference cells if their unaltered shape is helpful during alignment. The payload is encoded by means of single pixel shifts of the halftone clusters. The data carrying capacity of these examples are 447 and 349 bits, respectively, for the left and right examples in Figure 2. The payload is encoded in the Stegatone as shown in 3(c).

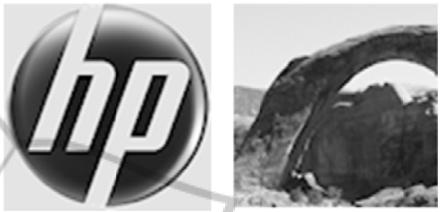


Figure 2.

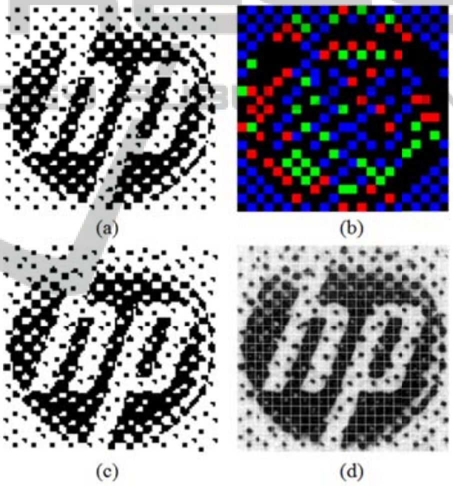


Figure 3.

2.2 Forensic Print Signature

The approach follows a methodology first proposed by Daugman in his 1993 paper on iris recognition and expanded on in subsequent publications (Daugman, 2006); (Daugman, 2007). This approach has become the backbone of many government and commercial biometric recognition systems; offering, as it does, the ability to robustly discriminate many billions of iris patterns.

Iris recognition differs from the Stegatone authentication task in three important regards. First, our images are captured using a specialized contact imaging device DrCID (Dyson Relay CMOS Imaging Device; Adams, 2010) at an almost fixed high resolution (about 7900dpi), whereas iris images are captured using traditional optics and thus vary in size over a small but significant range. Second, parts of the iris are not properly imaged due to either obscuration (by the eyelids or the eye-lashes) or specular reflections of the near-infrared light sources. Thus encoded features extracted from these regions must be robustly and accurately excluded from the statistical comparison process. Print images, on the other hand, do not generally suffer such imperfections and the whole of the encoded sequence can be used. Finally, unique iris features can be encoded across a wide range of spatial frequencies while the random perturbations associated with printed halftones are more limited.

For both Stegatone decoding and print signature extraction it is important to accurately and with good repeatability be able to register the captured Stegatone image as shown in Figures 3(d). In this work Stegatone patterns are registered using multi-scale gradient descent (Bouguet, 1999) derived from the well-established Lucas and Kanade (1981) method. For the multi-scale representation we normalize band pass filters (difference of successive Gaussian filtered images) to have unit standard deviation in order to minimize the difference between the stylized scaled (13x from 600 to 7900dpi) half-tone images and the printed and captured Stegatones that are closely related to them.

Following Daugman's methodology, the random signal is demodulated to extract its phase information using quadrature 2-D Gabor wavelets. In our case the Gabor filters use Cartesian coordinates and not the polar coordinates used for iris biometrics. That is

$$h_{\{Re,Im\}} = sgn_{\{Re,Im\}} \iint I(x,y) e_g . e_\omega \, dxdy$$

where

$$e_g = e^{-\pi[\![(x-x_0)^2/\alpha^2+(y-y_0)^2/\beta^2]\!]}, \qquad e_\omega = e^{-2\pi i\omega_0(x-x_0)}$$

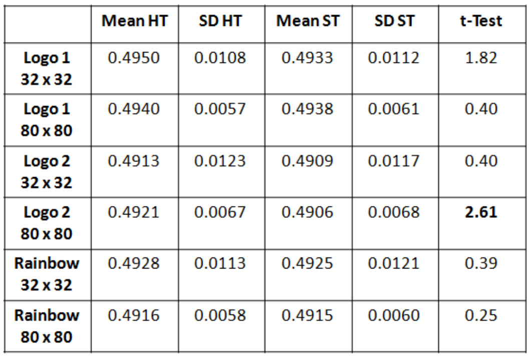
ignoring orientation: where $h_{\{Re,\ Im\}}$ is a complex valued bit whose real and imaginary parts are either 1 or 0 depending on the sign of the 2-D integral; *I(x, y)* is the warped raw image; α and β are size parameters of the Gaussian envelope; the parameter ω_0 is the spatial frequency of the filter. There is an additional orientation parameter θ_0 which is ignored in this formulation for simplicity. Thus, for all samples each wavelet provides two bits towards the phase encoding that describes the random elements of the printed halftone. Samples can be combined spatially over an *M* x *M* grid and through the choice of filter control parameters – notably frequency ω and orientation θ.

3 RESULTS & CONCLUSIONS

We have printed a number (>8) of identical halftone and Stegatone images on 3 identical HP4345 Laser Printers. There are two versions of an HP logo (labeled Logo1 and Logo2 with white and grey backgrounds respectively) and the Rainbow Bridge. Each print is captured twice (using different imaging devices) in order to compare the fractional Hamming Distance (HD) scores of valid matches with those of the binomially distributed statistically independent false matches.

First let's compare the statistical properties of Stegatone derived Gabor signature profiles with those derived from halftones as previously reported in Pollard *et al* (2012). The crucial difference is that the same digital halftone model is used to register both the halftone print (which was derived from it directly) and the Stegatone which includes small but significant deviations from the original halftone; which are unknown at the start of the decoding process. In Table 1 fractional Hamming distance statistics are compared for each of the three printed images. Each row represents false comparisons amongst all collected halftone (HT) and Stegatone (ST) images. For this test, there were 24 such images (276 comparisons) for all cases except the original Rainbow halftone images reported in the earlier paper for which there were 48 images (1128 comparisons). In every case, a single Gabor filter was used with λ = 8 pixels and two sampling densities *M* = 32 (which leads to a 2K bits/256 bytes code used for iris biometrics) and *M* = 80 (beyond which recognition rates were found to plateau). In all cases, except *M* = 80 for the second HP logo, the mean and standard deviations of Stegatone images compared to their halftone equivalents were sufficiently similar as to be considered the same within the 95% confidence limit of the t-Test.

Table 1: Hamming Distance Statistics.



	Mean HT	SD HT	Mean ST	SD ST	t-Test
Logo 1 32 x 32	0.4950	0.0108	0.4933	0.0112	1.82
Logo 1 80 x 80	0.4940	0.0057	0.4938	0.0061	0.40
Logo 2 32 x 32	0.4913	0.0123	0.4909	0.0117	0.40
Logo 2 80 x 80	0.4921	0.0067	0.4906	0.0068	**2.61**
Rainbow 32 x 32	0.4928	0.0113	0.4925	0.0121	0.39
Rainbow 80 x 80	0.4916	0.0058	0.4915	0.0060	0.25

The results in Table 1 show that the false match distribution statistics are not significantly altered by the change from halftone to Stegatone printing. This is not very surprising as the frequency content of each image type is significantly the same. Furthermore, the collection of false match statistics is not dependent on high accuracy registration and so is not likely to be affected by mismatch between the digital halftone used to register the Stegatone image. Of more interest is the effect this mismatch has on the Hamming distance of correct matches. Figure 4 shows a scatter plot of fractional Hamming distance for 20 correctly matching image pairs for the Rainbow Bridge Stegatone ($\lambda = 8$; $M = 80$) along with the (rotated) probability density function (PDF) for false matches. As can be seen clearly from this figure the probability of any of the correct matches being generated by chance is very low indeed. In fact the average z-score of false positives for the Rainbow Bridge is 57.95 which corresponds to a markedly small probability of $4\text{x}10^{-732}$.

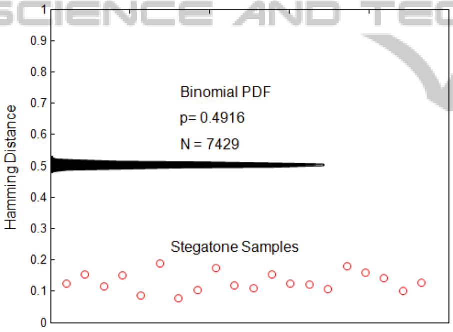


Figure 4.

Using the average z-score as a representative shorthand for the statistical robustness of the forensic print signature, Figure 5 compares halftone and Stegatone values for the conditions presented in Table 1. Robustness is clearly maintained for all conditions and image types. Note that the longer phase code ($M = 80$) results in much greater statistical robustness. This improvement can be increased further by combining extra Gabor filter frequencies and orientations.

Thus it is possible to use a single small 4mm square Stegatone print and capture with a high resolution imaging device to provide both covert data encoding (raw error rates for the best printer were 10%, 6% and 1% for the respectively for the Logo1, Logo2 and Rainbow stegatones) and a unique forensic print signature that exploits the stochastic nature of the print process and underlying surface substrate of the paper on which it is printed.

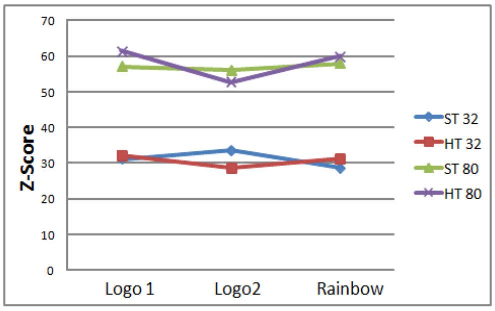


Figure 5: Mean z-scores for valid matches ($\lambda = 8$; $M = [32, 80]$) for both Stegatone (ST) and halftone (HT) image data.

Despite their modest size, Stegatones of this kind are able to encode considerable amounts of data; in fact the Rainbow Bridge example is able to robustly encode 256 bits which is at least comparable to the highest resolution 2D barcode of this size. In fact 2D barcodes rarely, if ever, encode more than 150 bytes per square cm, meaning a 4 x 4 mm barcode would be no more than 200 bits, easily outdistanced by the examples herein.

Using the Gabor phase coding approach halftones and Stegatones of this size are able to practically discriminate an almost infinite number of printed instances. While iris biometrics limited the code size to 2K bits, the high resolution (7200ppi) images used in these experiments allows us to greatly extend the code length (real and effective) through higher sampling frequency. In fact it is possible to increase this yet further by adding more independent Gabor components at other frequencies and orientations to achieve exceptional coding efficiency (albeit at greater memory requirement for the stored data).

REFERENCES

Adams, G., 2010, Handheld Dyson Relay Lens for Anti-Counterfeiting, *IEEE IST*.

Bouguet, J-Y., 1999, Pyramid Implementation of Lucas Kanade Feature Tracker: Description of the algorithm, *OpenCV Documents*, Intel Corporation, Microprocessor Research Lab.

Daugman, J. G., 1993, High confidence visual recognition of persons by a test of visual phase information, *IEEE PAMI, 15(11)*.

Daugman, J., 2006, Probing the uniqueness and randomness of IrisCodes: results from 200 billion comparisons, *Proc. IEEE, 94(11)*.

Daugman, J., 2007, New methods in iris recognition, *IEEE SMC, 37(5)*.

Lucas, B., Kanade, T., 1981, An iterative image registration technique with an application to stereo vision, *IJCAI*.

Pollard, S., Simske, S., Adams G., 2010, Model based print signature profile extraction for forensic analysis of individual text glyphs, *IEEE WIFS*.

Pollard, S., Simske, S., Adams G, 2012, Print Biometrics: Recovering Forensic Signatures from Halftone Images, *IAPR ICPR*.

Pizzanelli, D., 2009, *The Future of Anti-Counterfeiting, Brand Protection and Security Packaging V*, Pira International, Leatherhead, UK.

Ulichney, R., Gaubatz, M., Simske, S., 2010 Encoding information in clustered-dot halftones, *IS&T NIP26*.