COMPUTING
SCIENCE

Printer Identification Techniques and Their Privacy Implications

John Mace

TECHNICAL REPORT SERIES

No. CS-TR-1211    July 2010
Abstract

This paper explores current printer identification techniques which allow the origins of a printed document to be established. The printer used to create a particular document can be traced by using unique and hidden information contained within that document. Printer identification can ultimately lead to the printer’s owner(s) which provides a valuable tool to government agencies during criminal investigations involving forged documents or associated correspondence. Two groups of printer identification technique are examined. Passive techniques utilise microscopic flaws in a document’s print for printer matching while active techniques explicitly embed traceable data into a document. Evidence has emerged to suggest that embedding tracking data into printed documents has been employed since the 1980s. No legal precedents need be followed to obtain and use hidden tracking data nor does the public have to be informed of this practice. Related privacy concerns are discussed brought about by the potential to compromise the anonymity of every single printed document.
Abstract

This paper explores current printer identification techniques which allow the origins of a printed document to be established. The printer used to create a particular document can be traced by using unique and hidden information contained within that document. Printer identification can ultimately lead to the printer’s owner(s) which provides a valuable tool to government agencies during criminal investigations involving forged documents or associated correspondence. Two groups of printer identification technique are examined. Passive techniques utilise microscopic flaws in a document’s print for printer matching while active techniques explicitly embed traceable data into a document. Evidence has emerged to suggest that embedding tracking data into printed documents has been employed since the 1980s. No legal precedents need be followed to obtain and use hidden tracking data nor does the public have to be informed of this practice. Related privacy concerns are discussed brought about by the potential to compromise the anonymity of every single printed document.

About the author

John Mace is studying for a PhD in the School of Computing Science at Newcastle University, under the supervision of Prof. Aad van Moorsel. John completed a Batchelors degree in Computing Science at Newcastle University in 2010.

Suggested keywords

PRINTER IDENTIFICATION
TRACKING DOTS
PRIVACY
Printer Identification Techniques and Their Privacy Implications

John C. Mace
School of Computing Science,
Newcastle University, UK
j.c.mace@ncl.ac.uk

Abstract. This paper explores current printer identification techniques which allow the origins of a printed document to be established. The printer used to create a particular document can be traced by using unique and hidden information contained within that document. Printer identification can ultimately lead to the printer’s owner(s) which provides a valuable tool to government agencies during criminal investigations involving forged documents or associated correspondence. Two groups of printer identification technique are examined. Passive techniques utilise microscopic flaws in a document’s print for printer matching while active techniques explicitly embed traceable data into a document. Evidence has emerged to suggest that embedding tracking data into printed documents has been employed since the 1980s. No legal precedents need be followed to obtain and use hidden tracking data nor does the public have to be informed of this practice. Related privacy concerns are discussed brought about by the potential to compromise the anonymity of every single printed document.

Keywords: Printer Identification, Tracking Dots, Privacy

1. Introduction

With an ever decreasing cost of high quality printers, the printed ‘document’ has become commonplace. A ‘document’ is considered to be a piece of printed matter that provides information, such as passports, driving licences and banknotes. Today, printed documents are frequently associated with many criminal and terrorist acts, be it counterfeiting, forgery or copyright infringements. With the continuing improvements in printer and scanner technology, these individuals are able to produce very high quality fake documents, which are increasingly harder to detect when compared to those created using more traditional forgery techniques. Criminals can now digitally scan currency and print counterfeit money, or use similar techniques to produce forged ID cards, airline boarding passes and official documents, for example.

A valuable tool to government agencies is the ability to verify a document’s authenticity and trace those responsible for producing exposed fakes. One way of verifying a ‘true’ document is to link its production with a known and authorised printer. Providing such a mechanism would uncover forged or altered documents and potentially provide evidence that a suspect printer held as part of a criminal investigation produced those documents. The printing of genuine documents could be done in a secure and confident manner with the knowledge that any attempts to forge or copy those documents will be detected. Such a link between document and printer however, means not only establishing which type and model of printer was used but also which specific printer was used. Authorities must be capable of differentiating between documents printed on two different printers of the same model.

Tracing a printer’s whereabouts from the criminally connected documents it creates (e.g. forgeries or printed correspondence) could potentially lead to the criminals themselves. Once the offending printer is identified, its location and that of its owner may be done via the printer’s retailer, providing they retain sales records, or from the owners themselves if they provide their printer’s manufacturer with registration and warranty information.

The area of printer identification is an active research problem being carried out at a number of institutes, notably Delp et al at Purdue University in the US [1]. From this research, two printer
identification techniques have been suggested to address the issues previously mentioned: ‘passive’ and ‘active’. Passive techniques analyze a document’s unique characteristics and match them to those of a known printer, so providing the required link. Active techniques explicitly embed hidden printer specific information into a document to enable printer traceability.

Unbeknownst to millions of printer users, an active printer identification scheme has been employed by the US and other governments since the late 1980s. This scheme, carried out in conjunction with the majority of printer manufacturers has been used to trace printers used in criminal activities. Having recently been uncovered by the Electronic Frontier Foundation (EFF) [2], the addition of ‘secret codes’ to documents created by both criminals and innocent users has raised many human rights and privacy concerns.

This paper discusses current printer identification research and techniques (both passive and active) including the covert scheme already used notably in the US, followed by privacy issues, potential drawbacks and concluding remarks.

2. Identification techniques

A need has been identified for government agencies to be able to authenticate and/or trace the origins of printed documents. Documents can be deemed genuine by certifying their creation is from a known and authorised printer, while tracing the origins of fake or copied documents may potentially lead to criminal groups. Traditional methods of authenticating and tracing documents, for example, special ink, holograms and threads in banknotes are limited due to expense and the need for specialist equipment. A more accessible way of ascertaining the origin of a document is to identify the specific printer used to create it. A number of techniques have/are being developed using passive and active techniques.

2.1 Passive techniques

Passive techniques analyze a document’s unique characteristics and match it to those of a known printer. This technique can be used to authenticate a genuine document or match a document with a suspect printer, held as part of a criminal investigation. These unique characteristics come from the fact that no two printers are or behave the same. When manufactured, every printer will inherit unique imperfections and characteristics from the components used to construct it. These mechanical parts used to build printers, including printers of the same model are not 100% the same and would be far too expensive to be so. Therefore, printers produce documents with specific defects, which can be analyzed and used to tie those documents with their printers.

Delp et al describe a number of passive techniques to identify laser or “electro-photographic” (EP) printers from printed documents [6]. In [4], the print quality defect called ‘banding’, which produces horizontal imperfections in the document, is utilised for this purpose. Banding occurs in printers whose print mechanism includes a rotating drum coated with a charged material that releases its charge when exposed to light. A laser moves along the drum selectively removing the charge in certain areas, which in turn attracts print toner to form letters or image features. The toner is then transferred onto the paper to form the document. The speed at which printer drums rotate is variable so any slow down causes darker print, while speeding up causes lighter print. This results in alternate horizontal bands of dark and light print as seen in the bottom image of figure 1. The frequency

Figure 1: The effects of banding (bottom picture)
of these bands can be analysed using mathematical techniques to obtain an intrinsic signature that is matched with known printer banding frequencies stored in a database. This allows the make and model of the printer, which produced that document, to be identified. Although specific printers cannot be currently identified, initial results show that banding frequencies are stable enough to use as an intrinsic signature to determine a printer’s model and manufacturer.

While banding frequencies are easy to determine in documents displaying large mid-tone regions, they are hard to detect from text. In [3], a technique using image texture analysis is described by Delp et al to identify a printer from small regions of a document such as individual text characters. The imperfections in a printer, causing fluctuations in the amount of toner transferred to the document, are modelled as a texture, providing a set of unique features for identification purposes. First, a document is scanned before all the letter ‘e’s are extracted, ‘e’ being the most common character in the English language. Using analysis tools, a set of unique features is extracted from each character to form feature vectors for each ‘e’. These feature vectors are classified individually by comparing them to 5000 known feature vectors, with majority voting deciding the final classification. This technique successfully classified 9 out of the 10 printer models tested, but as in [4], will only determine a printer’s make and model. Also, it is restricted to text from a laser printer and does not encompass documents containing colour and/or images nor does it classify documents produced on inkjet printers.

In [5], Delp et al extend their work in [3] by using varied font size, font type, paper type and printer age; and the effects these variables have on printer identification. A document is scanned and a set of features extracted from each character ‘e’ as with the technique previously described. These sets of features form feature vectors which are individually classified using a modified classification method employing a support vector machine (SVM) as described in [7]. Using an SVM provides better generalization and was able to correctly classify all 10 of the test printers by make and model when variables such as font size and type were the same in both the document and the comparison data. When document and comparison data variables differ, printer identification is not 100% correct. For example, when there is a difference of 2 points between fonts, correct identification is 90% while an 8-point difference yields only a 40% success rate. Further work is currently being carried out to improve printer identification results when taking into account different fonts, paper types and printer age.

Work carried out by Deng et al [8], investigates the identification of laser printers based on matching printed character shapes. Due to print overspray, character edge raggedness, toner density, etc., a single character can have a different ‘shape’ when produced by different printers. The identification technique involves three distinct steps; image acquisition, image pre-processing and character matching. Image acquisition uses specialist equipment to obtain microscopic images of characters contained within a document. Pre-processing involves various techniques such as extracting certain characters, removing ‘noise’ and obtaining binary images. These normalized characters are then matched with characters from documents of known origin, held within a database. This matching technique uses distance transform [9], a method widely used in pattern recognition and image matching. The algorithm used is able to determine the closest matching printer or printers to that which created the suspect document even from a group of same make and model printers. Initial results give an identification accuracy of 25% when selecting a single candidate printer and 82% when selecting a set of five candidate printers. Further work is being carried out to extract further intrinsic printer features thereby improving the identification accuracy.

Similar work is done by Oliver et al [10] who use an ImageXpert print quality analyzer [11] to obtain unique signatures, which may be used for printer identification. Test patterns are generated by printers using various ‘impact’ and ‘non-impact’ technologies including ink jet and laser printing. These test patterns, made up of text, lines and dots, are evaluated using the ImageXpert analyser to determine various print metrics such as

![Figure 2: Vertical lines printed by Canon, Epson and HP printers](image-url)
character raggedness, over-spray, dot roundness and satellite drops. Satellite drops are seen under magnification and can be considered to be small drops of ink deposited on the page outside the perimeter of a printed character. An illustrated example (fig. 2) shows the differences between three ink jet printers from three different manufacturers, Canon, Epson and HP. On analysing printed vertical lines the Canon printer displays noticeable raggedness on the right side of the line, while the HP printers shows a degree of overspray on the left hand side. The Epson printer shows neither of these traits. By comparing such derived metrics against those of known print patterns, the type and make of printer can be established. From the careful selection of appropriate metrics and print features, further work sees the possibility of differentiating between individual printers of the same make and model. Complementary analysis of the effects in paper, ink and toner choices will also be made.

In [12], Kee et al create printer profiles by modelling the geometric degradation in a document caused by printing. This technique allows both the linking of a document to a printer and the detection of document inconsistencies for authentication purposes. The construction of a printer profile and the subsequent printer identification is carried out via three distinct steps. First a document is digitally scanned from which all matching characters are located, for example, all the letter ‘a’s. Once all the characters are correctly aligned and processed, the second step is to construct a printer profile using a principal components analysis (PCA) [13] thus providing a model capturing complex degradations in the print. The third and final step is to use the printer profile for printer identification by matching it with profiles of known printers. Ten printers were tested, each producing documents containing 22,400 characters all of which were processed to create the required profile. For each of the ten documents created, identification of its original printer was near perfect even between printers of the same make and model. However, these results are only achievable by creating profiles for differing toner levels. Future work seeks to remove this toner level dependency and make the identification technique more sensitive for the same make and model of printer.

Many additional studies have been more recently undertaken (e.g. [14-17]), using similar techniques as those previously described and yielding comparable results.

2.2 Active techniques

Active techniques explicitly embed hidden information into a document allowing that document to be matched with its printer. This information may be covert data unique to a document’s printer or it may be the introduction of deliberate yet known imperfections into the document’s text and/or images. Unlike passive techniques, the suspect printer typically does not need to be in possession of the investigators for a match to be made. Purchasers may provide their details when buying a printer or when registering a printer with the manufacturer for warranty purposes. Such a process will typically tie an individual printer to its owner. Therefore if a document contains information unique to an individual printer, that printer can be traced to its owner via the information held by the printer manufacturer. Because a printer will embed unique information into the documents it produces, the accuracy rate for printer identification is significantly higher than the current passive techniques previously described. For active techniques to be wholly effective, the embedding of data and its subsequent use must be kept secret while the hidden data itself remains undetectable to the naked eye.

In [25] and [26], Delp et al explore the use of the print quality defect ‘banding’ [4] to introduce an extrinsic signature into a document. In previously described passive techniques, implicit banding frequencies (fig. 1) are compared with known printer profiles to match document to printer. With the active method, printer unique banding is purposely introduced into the document allowing that document to be easily matched with its individual printer. The extrinsic signature is embedded into the document by modulating the printing process, notably the laser exposure, which in turn generates the banding signals on the printed page. By varying the modulation, artificial banding of different frequencies can be introduced into a document’s text and images without perceptual degradation of print quality. To be effective, this technique requires the printer hardware to be modified, particularly the print mechanism, which will potentially prevent any attempts to modify the hidden data before it is printed. To detect the extrinsic signature and match it to a printer, the tools developed for passive printer identification are used. Initial results show minimal reduction in print quality although due to
limitations imposed by the main printing drum, banding frequencies no higher than 50 cycles or ‘bands’ per inch have been achieved. Future work aims to increase banding frequencies to over 100 cycles per inch thus providing a document with no visible decline in print quality and rendering the embedded information undetectable to the naked eye.

Gaubatz et al [27] propose a quality assurance (QA) system associated with printed security markings for performing printer identification. The use of colour tiles (fig. 3) was proposed in a previous work [28] as a security mechanism to deter counterfeiting and aid in document authentication. Here these tiny colour tile deterrents are added to a document and utilised to implement document and printer matching. A unique identifier is encoded in a printed tile by setting each of its 56 sub-regions to one of six different colour combinations. Device authentication is achieved when a candidate device is capable of decoding the unique identifier. A 10-feature vector is formed from the printed tile using various metrics used to predict the outcome of the authorisation procedure. When identifying the document’s printer, a classifier is used to compare the features of a printed tile’s feature vector with digital representations of the original deterrent produced by suspected printers. This technique lends itself to both active and passive techniques; active by explicitly embedding data into a document and passive by matching the printed result with profiles of known printers. Preliminary testing has produced results which yield printer detection accuracy comparable to other approaches suggesting that precise identification is possible. Future work will investigate further algorithmic classification methods to improve printer identification accuracy.

Unknown to many printer users, an active technique of printer identification has been in use since the 1980’s. Printers from several of the main printer manufactures explicitly encode tracking data into every document that is created [19]. Found in documents from colour laser printers and photocopiers, this data takes the form of microscopic yellow dots repeated across the entire page and arranged within a grid. This makes it impossible to circumvent the system by printing in just a small area of a document or by attempting to cut away certain sections. The grid is capable of encoding up to 14 seven-bit bytes of tracking information, presented in rows and columns of dots. The millimetre sized yellow dots (fig. 4) appear approximately every inch within a document and are situated amongst the printed text and images. Yellow is chosen for the dots as this makes them invisible to the naked eye when printed on a white background.

The dots are arranged to form codes or tracking data whose make-up can differ between printer manufacturers. Several companies reportedly encode the serial number of the printer, the date and time of the printing together with other such data. Canon, which fit the tracking mechanism to all their colour laser printers, encodes the country and dealer the printer was delivered to, within a unique number added secretly to each page [18]. The dots themselves are embedded into the document at approximately 20 billonths of a second before printing, by means of a computer chip located near the print mechanism. Viewing such embedded dots can be done by shining a blue LED torch on to the document which must be inspected closely through a magnifying glass. It can be imagined that the embedded tracking data is decoded using secret and proprietary algorithms known only to the printer manufactures and other associated parties.

This printer identification technology was first developed 25 years ago by Xerox to allay the fears that coloured printers would be used to produce counterfeit currency. It is reported in [19] and [20] that the US government were party to this technology development and now use it as standard practice in criminal cases involving printed documents to trace the printer used and ultimately the wanted perpetrators. However, the addition of traceable data in potentially every document that is printed raises a number of privacy concerns as discussed in section 3.
3. Privacy Implications

The 2004 report by PC World magazine [20], together with further investigation by the Electronic Frontier Foundation (EFF) [21] brought to light the fact that embedding tracking data into printed documents was taking place in the US. Printer manufactures, on the request of the US government, commonly fit laser colour printers with devices that embed arrangements of yellow dots into all documents (see section 2.2). The US secret service then use this covert data, with the aid of the printer manufactures, to trace counterfeiters and other felons by the documents they produce during their criminal activities.

This practice between the US secret service and the printer manufactures has been in operation since the 1980’s. However, reports suggest that this technology is used outside the US and is employed by other governments (e.g. [18]). Described as a counterfeit deterrence, the US government stress that the identification and tracking of printers is done on a case by case basis and is used only for suspected documents as part of a criminal investigation [20]. It is unclear who generates the embedded tracking codes and who can decipher them, be it the printer manufacturers, the creators of the coding ‘chips’, the US government or a combination of these. A scenario can be imagined where the make and serial number is obtained from a document and the corresponding printer company contacted who hold information relating to the printer’s purchaser. Typically, electrical retailers retain purchaser information during a sale or via customers taking up warranty offers. Certain countries, for example China, keep a tight rein on the ownership and purchasing of electrical equipment such as printers, so recording information on every customer is done as standard. A printer company will typically maintain all customer information within a database whose content could be made available to government agencies upon request.

The US government state they only use the document tracking information to investigate criminal acts, but is this truly the case? Currently no law or statute exists in the US preventing the government from using this technology for other purposes, nor are there any laws to say what documents can or cannot be traced. This leaves a situation where the government cannot be made to adhere to the technology’s proper purpose or verify that no other use is taking place. In the current political climate it is not hard to imagine the US government using it for other purposes. One unanswered question is how many countries are employing this printer identification process? With reports emerging about its use in the US and Holland, the answer is likely to be many.

Those within the printer industry have known about the embedding of data into documents for years but have not had to notify customers of this feature. Therefore, despite some reports appearing in major publications, for example The New York Times [22], the use of this technology remains largely unknown to the public. Those that are aware are left with no choice in whether the data is added or not, as the feature cannot be disabled without the likelihood of breaking the printer. This tracking technology is not just aimed at those with expensive, ‘state of the art’ colour laser printers as it is appearing in printers of all price and quality brackets. For those printers who have been identified not to embed the yellow tracking dots [23], it is possible that some other kind of tracking information is included in a way as yet undiscovered. Its age and relative simplicity could indicate that it has been replaced by a more sophisticated system especially now the current coding system has been revealed.

The implementation of this tracking technology has been carried out with virtually no public awareness much less public discussion of the privacy and anonymity risks to printer users. It must be realised that through their use these secret codes could potentially track any document back to the person or business that printed it. Embedding hidden information into a document without knowledge or consent means an act presumed private could easily become public. Does this mean people can no longer conduct their private life or discussions as they otherwise would? Is the use of such technology an abuse of people’s entitlement to protect personal data? In fact isn’t this practice a blatant violation of human rights?

Printed documents have become an important tool for free speech with anonymous self publication and distribution of such material remaining a vital political communication channel in many countries. With the right to speak anonymously being threatened, long protected forms of expression could be in
danger. People, who print political pamphlets, membership lists and organize legal protests for example, could be in danger of being traced. Whistleblowers, dissidents and journalists amongst others could be at risk when printing documents especially when doing so in more oppressive states. With no laws in place there is nothing to stop privacy violations by governments and other organisations that have access to this printer identification technology. A government needs to follow no legal process to obtain and use any embedded document data, nor must they inform members of the public they are being ‘spied’ upon. What is to stop a government to share any information they gather with other states to help identify speakers? Is tracking information really used for tracking alone or is it also used as a form of surveillance? And what other deals have been done between governments and technology manufactures regarding secret tracking devices?

The practice of embedding hidden data into documents is reportedly for the tracking of criminals. But what is to stop criminals, who gain access to this technology, using it to their own advantage? Criminals could potentially trace and verify the owner of stolen and potentially embarrassing documents, and use that knowledge for blackmail purposes. Advocates against this technology (e.g. [24]) wish that documents were less traceable and users had better options to achieve anonymity. Although it would not guarantee absolute anonymity, as other methods are available (e.g. passive identification techniques), these campaigners would like to see a ban on traceable printers.

4. Potential drawbacks

In its current guise the notion of printer identification appears to present a number of shortcomings. Passive techniques identify and use the unique characteristics of a document to match it with a printer. These characteristics are typically imperfections in the document’s text and images produced by tiny flaws in the printer’s components. The current research in this area, as previously described, is far from accurate. The existing techniques require the printer to be in possession of the authorities for testing purposes or a profile of that printer to be held in a database. This would suggest a profile must be constructed and stored for every printer currently in existence for this identification technique to be wholly effective. If a printer profile is not held then a printer will be selected that is the closest match, in other words, the wrong printer. This technology is able to successfully determine between printer types (e.g. laser, inkjet) and between printers makes and models but cannot currently differentiate between printers of the same model. Factors such as different fonts, paper and print cartridge levels, which can affect the level of printer identification accuracy are being investigated. Passive techniques yield promising results but are by no means as accurate as the active process of explicitly hiding data within a document.

Active techniques purposely embed traceable information into a document, be it imperfections in text or images, or microscopic tracking dots encoding the printer’s serial number. These tracking dots are yellow in colour printed against a white background, making them appear invisible to the naked eye. However, this technique is reportedly only used with colour laser printer which limits its application dramatically. A large number of documents do not require colour and may be printed using a ‘greyscale’ facility. Furthermore, what is the percentage of documents printed on laser printers when cheaper alternatives are available, especially in the home? And what are the effects of using different coloured paper? Do the dots then become visible?

The idea of embedding hidden information into a document brings a number of potential avoidance mechanisms. It must be remembered that “baddies in security are arbitrarily smart” (Yan, 2010) and are likely to sidestep document tracking technology, especially now that increasing reports are emerging. A criminal may be an organisation ‘insider’ and use company printers or they may use publicly available printers in libraries and the like. With multiple users accessing a printer the possibility of tying individuals to particular documents is practically zero. Some organisations may require users to enter a password into a printer before its use, but this practice can be easily bypassed. A criminal could print the documents they require before discarding the printer, or steal a printer just for the purpose of creating those same documents. Furthermore, the criminal could simply avoid using a printer known to include printer identification technology, as listing in readily available reports (e.g. 23). Another
approach could be to somehow add yellow dots of their own to a document thus rendering the genuine tracking dots, and the information they encode, useless.

One method described for tracing the owner of a suspect printer is from information held on the owner by the printer manufacturer. This information is typically gained from product registrations. But how many people actually register a product they buy? Certainly not a criminal. Many states do not enforce compulsory product registration but even if they did, a purchaser could quite easily supply bogus information.

5. Conclusion

The basic premise of printer identification is to allow law enforcement agencies to trace the origins of fraudulent and/or incriminating documents held as part of a criminal investigation. Tracing a document’s printer will ultimately lead to the printer’s owner and potentially the criminal(s) being sought.

Two methods of printer identification have been described, passive and active, and the research being undertaken in these areas. The revelation that an active technique of embedding traceable information into documents within the US has also been discussed together with the privacy concerns this brings. The embedded information takes the form of microscopic yellow tracking dots which encode the printer’s serial number, printing timestamp and such amongst the text and images of a document. This practice has reportedly been adopted for years by US government agencies without any legal precedents and may potentially be taking place in many other countries.

The concept of tracing criminals via documents and the printers that create those documents has its merits. But as previously discussed, printer identification in its current guise is not perfect and brings many potential shortcomings particularly with the issue of privacy. If government agencies are going to use (or keep using?) such technology they must do so with the aim of preventing counterfeiting etc. while protecting privacy at the same time. They need a way to track criminals without compromising the anonymity of every single document that is printed.

References

2. EFF, “Electronic Frontier Foundation”, http://www.eff.org/, last visited 05/04/10
http://cobweb.ecn.purdue.edu/~prints/publications.shtml, last visited 06/04/10

7. C. W. Hsu, C. C. Chang, C. J. Lin, “A Practical Guide to Support Vector Classification”, National Taiwan University, Taiwan, 2003

8. W. Deng, Q. Chen, F. Yuan, Y. Yan, “Printer Identification Based on Distance Transform”,
Proceedings of 1st International Workshop on Intelligent Networks and Intelligent Systems (ICINIS ’08), Wuhan, China, 2008


10. J. Oliver, J. Chen, “Use of Signature Analysis to Discriminate Digital Printing Technologies”,
Proceedings of SPIE International Conference on Optical Security and Counterfeit Deterrence Techniques, 2004


14. O. Bulan, J. Mao, G. Sharma, “Geometric Distortion Signatures for Printer Identification”,
Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Taipei, Taiwan, 2009


18. W. De Vries, ITworld, “Dutch track counterfeits via printer serial numbers”,
http://www.itworld.com/041025dutchprinter, last visited 21/04/10


http://www.pcworld.com/article/118664/government_uses_color_laser_printer_technology_to_track_documents.html, last visited 23/04/10

http://www.eff.org/issues/printers/, last visited 21/04/10


Bibliography


• B. Byfield, Linux Journal, “Seeing yellow over color printer tracking devices”,
  http://www.linuxjournal.com/node/1000247, last visited 23/04/10

• D. O’Brien, Electronic Frontier Foundation (EFF), “EU: Printer Tracking Dots May Violate
  Human Rights”, http://www.eff.org/deeplinks/2008/02/eu-printer-tracking-dots-may-violate-human-rights, last visited 23/04/10

• S. Schoen, “Decoding Identifying Printer Information”, Proceedings of Chaos Communications
  Camp (CCC), Finowfurt, Germany, 2007

• L. Weinstein, The Privacy Forum, Ids in Color Copies – A PRIVACY Forum Special Report”,
  http://www.vortex.com/privacy/priv.08.18, last visited 23/04/10