TRACES OF FORGERY IN DIGITALLY MANIPULATED DOCUMENTS

Audrys DERINGAS
Institute of Forensic Examination, Vilnius, Lithuania

ABSTRACT: Criminals use modern technology for producing counterfeit documents. The counterfeit system (scanner, computer, printer) can be successfully used by criminals for the production of banknotes, invoices, contracts, diplomas, etc. In the process of production of these documents the graphic programmes are often used for changing some details such as signatures, seal impressions, numbers and other important information. Law enforcement agencies are often interested in not only if the document is counterfeited, but in the identification of the source document. This is more difficult when the counterfeit has changes made by graphic programmes, as these programs can alter the document to an almost unrecognisable state. The paper focuses on the possibilities to detect the traces of alterations made by graphic programmes in questioned documents. The report is illustrated with pictures from case work.

KEY WORDS: Questioned documents; Digital images.

Problems of Forensic Sciences, vol. XLVI, 2001, 375–382
Received 14 December 2000; accepted 15 September 2001

INTRODUCTION

In my previous presentations [1, 2] I discussed the possibilities of using digital images in questioned document examination, their usage in European forensic institutions and attitudes toward this examination technique. This report is devoted to opposite problem – the use of digitally manipulated images for counterfeit document production by criminals and challenges to questioned document examiner concerning the problem.

In industrial countries computer systems are becoming as common as televisions or telephones. The equipment quality gets better and better. Printers and scanners have higher resolution, expanded printing possibilities. Computers are faster and with great memory resources. Having such devices, it is tempting to make counterfeits, for example, banknotes. This tendency can be illustrated by statistical data [3] from USA Secret Service (Figure 1): the percents of inkjet printed US dollars in 1995 were 0.5%, in 1999 – 40% and in the first month of 2000 – 46%.

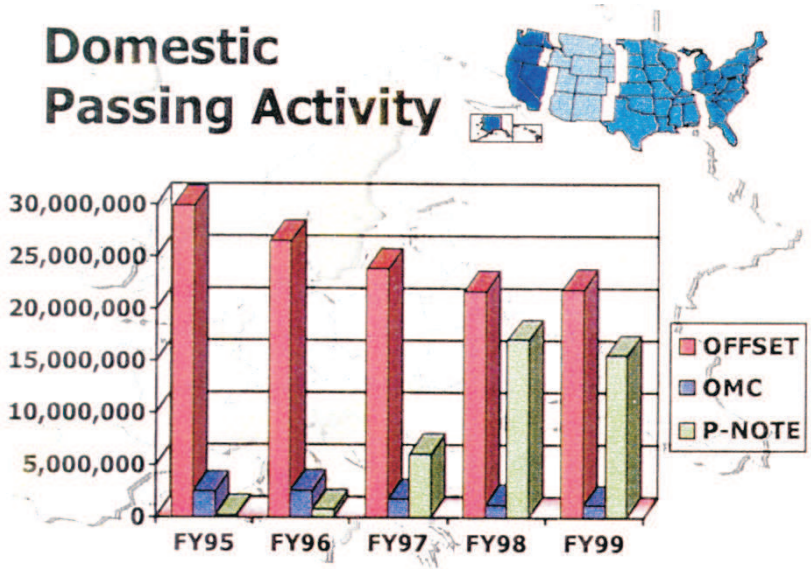


Fig. 1. The tendencies of counterfeiting USA currency in 1995–1999 (OMC – office machine copiers, P – printers).

In a way, producing banknotes is the simplest case. Using modern equipment, a more complicated process would be to write contract text by means of computer, insert seal impressions with signatures scanned from other documents, print the contract, copy with low quality equipment, fax it, and go to the bank for several thousands of dollars. After such a process finding traces of forgery is almost impossible. Trash marks of low quality copying and fax distortions covers possible traces of forgery. In this case revealing counterfeit was possible because documents with genuine seal impressions and signatures were available. The configuration of signature and position in respect to seal impression was identical to the faxed contract and a comparative document.

Presently the market is full of various powerful graphic programmes: Photoshop, CorelDRAW, ImagePro, etc. In spite of different names they all have one general feature in common: they are created to manipulate images. An image or its details can be erased, cut, copied, replaced, painted, coloured and changed in many different ways. These features can be successfully used by criminals for the production of banknotes, invoices, contracts, diplomas and other documents. In the process of production of these documents graphic programmes are often used for changing some details such as signatures, seal impressions, numbers and other important information. Law enforcement agencies are often interested in not only if the document is counterfeited but in the identification of the source document. Thus arises the problem of detecting the digitally altered document.

First of all, it is worthwhile to mention that in these cases we will not find traditional traces of alteration such as a change in paper thickness, rough up paper fibres, or different luminescence. However, not all traces are absent. We can find foreign elements, imperfection of details, or drawn elements. The possibilities of finding traces depend on the skills and scrupulousness of criminal, and, certainly, on the same qualities of the document examiner.

The following is some cases from practical examination work, where documents were digitally manipulated.

SEAL IMPRESSION AND SIGNATURE

In Figure 2 we can see a questioned seal impression and suspected original from which the questioned impression was copied. First of all, we can observe that the position of the questioned impression according background and printed text "Vilnius, 19" is identical to the suspected one. The next step is to examine the handwriting position place in the questioned impression. The magnified fragments of the questioned seal impression and suspected original are presented in Figure 3 a, b respectively. Analysing the word "RESPUBLIKA" we can see some foreign elements, irregular forms of some letters ("S", "I", "K"), and the star in the questioned impression is also irregular. If the image of the questioned seal is scanned to "PhotoShop" and viewed in CMYK mode black channel, the black dots of irregular shape are evident. I hope the presented evidence is enough for definite conclusion, that the questioned seal impression was scanned from the suspected original, digitally manipulated and printed again.

a b

Fig. 2. Questioned seal impression (a) and suspected original (b).

a

b

Fig. 3. Fragments of questioned seal impression (a) and suspected original (b).

RECONSTRUCTED BACKGROUND

In Figure 4 we see a digitally reconstructed background. The most probably in the place where some data were written. In the central part blue lines have a break and are not continuous. In the right upper side the yellow line is broken. Therefore, the attempt to mask removed data is not very successful.

NUMBERS

Figure 5 shows changed numbers. The traces of "box" around last figures "99" are noticeable. Judging from the background around these figures we can conclude that the first and fourth nine were not used for the last nines.

Fig. 4. Manipulated background.

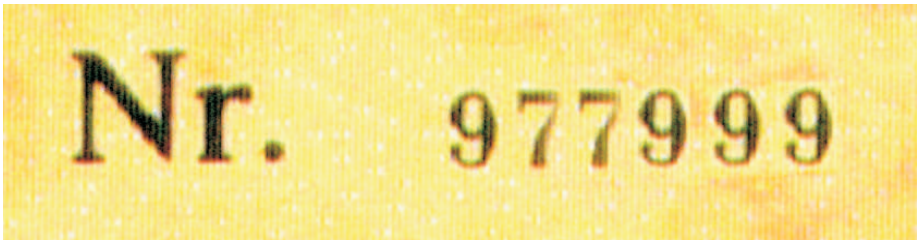
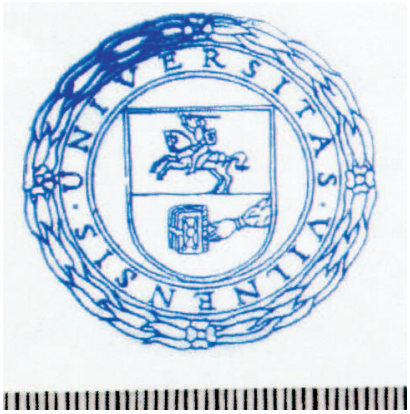


Fig. 5. Manipulated numbers.

RECONSTRUCTED SEAL IMPRESSION

Figure 6 shows three seals impressions in a – questioned, b – suspected original, c – comparative. The richer inking in the upper part of the questioned and suspected seal impressions indicate that the questioned impression was copied from the suspected one. However, what is the fate of the signature? In Figure 7 we see magnified fragments of the seal impressions in the position of the signature. Some characteristics show the removal of the signature in Figure 7 a: breaking of the vertical line on the right, and remains of signature between two parallel rounded lines in lower part of the picture. We find the strongest evidence of manipulation with the seal if we compare the left outer pattern of the questioned seal with the comparative impression. We can easily notice pattern differences in the seal impressions: the "flowers" are different. This case shows the imperfection of criminal work and not paying attention to details, which are substantial for the questioned document examiner.

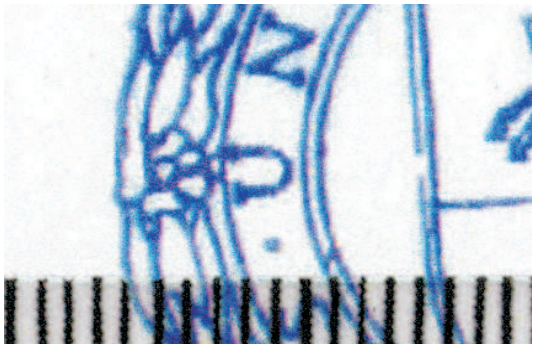


a

b

c

Fig. 6. Questioned seal impression (a), suspected original (b), comparative impression (c).



a

b

c

Fig. 7. Fragments of questioned seal impression (a), suspected original (b) and comparative impression (c).

CONCLUSIONS

After discussing the materials presented above, the key question must be asked: what is the evidence that these documents were namely digitally altered? Maybe the original document was colour copied, alterations made "by hand" in the photocopy and altered document was copied again. It is not very strong evidence of digital manipulation. The quality of alteration, factual information about circumstances of the case and intuition can be hints to distinguish ordinary alteration from the digital one. On the other hand, sometimes it is enough to confirm the very fact of alteration. Nevertheless, we can conclude about advantage in counterfeits production and spreading usage of graphic programs for it. These aspects complicate the questioned document examiner's task to recognise these types of forgery.

References:

1. Deringas A., Digital images in QDE, 4th International Congress of the Gessellschaft für Forensische Schriftuntersuchung (GFS), Hamburg 1999.
2. Deringas A., The possibilities of using standard PC Programs for QD examination, Joint Meeting of the European Conferences for Police and Government Handwriting and Documents Experts, Scotland, 1998.
3. Materials of Combating Economic Fraud and Counterfeiting Seminar organised by the United States Secret Service, Vilnius 2000.