Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Martin Steinebach
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-349
Fax 06151 869-224
martin.steinebach@sit.fraunhofer.de
www.sit.fraunhofer.de

FORSICHT

IT-FORENSISCHE SICHTUNG VON BILD- UND VIDEODATEIEN

Ermittler bei Polizei und Staatsanwaltschaft müssen oft auf der Suche nach illegalem Foto- und Videomaterial große Mengen von Daten sichten. Dazu benutzen sie Methoden und Werkzeuge der IT-Forensik. Das Fraunhofer SIT hat mit dem Projekt ForSicht diese Methoden erweitert und verbessert sowie das Durchsuchen der Datenmengen signifikant beschleunigt.

Polizeibehörden untersuchen große Datensammlungen oft mit IT-Werkzeugen, um illegales Material aufzuspüren. Meist handelt es sich hier um kinderpornographische Bilder und Filme. Herkömmliche Werkzeuge erkennen kinderpornographische Dateien nur dann zuverlässig, wenn eine identische Kopie des Bildes bereits in einer Datenbank hinterlegt ist. Über einen eindeutigen Vergleichswert, einen sogenannten kryptographischen Hash, kann die Software diese Kopie automatisch zuordnen und identifizieren.

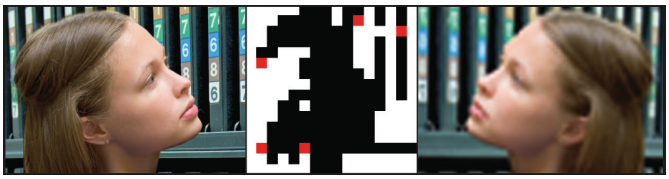
Die Schwäche dieses Verfahrens ist, dass selbst minimale Veränderungen an der Datei den Hashwert verändern. Wenn ein Nutzer beispielsweise ein Bild oder eine Videodatei in ein anderes Datenformat umwandelt, ist der Hash soweit verändert, dass eine Identifizierung über dieses automatische Verfahren nicht mehr möglich ist. Das bedeutet, dass Polizeibehörden derzeit mit dieser Technik nicht in der Lage sind, bewusst verschleiertes illegales Material aufzuspüren. Die Ermittler müssten also zusätzlich selbst die Datensammlungen sichten, um sicherzugehen, dass tatsächlich alle illegalen Dateien gefunden werden.

Eine Alternative beziehungsweise Ergänzung zu diesen etablierten Mechanismen sind sogenannte robuste Hashverfahren. Diese Technik nutzt nicht eine mathematische Funktion auf den Binärdaten einer Datei zur Identifizierung, wie es bei kryptographischen Hashes der Fall ist, sondern orientiert sich an der menschlichen Wahrnehmung: Wenn ein Bild für das menschliche Auge identisch oder sehr ähnlich erscheint, ist auch der Vergleichswert identisch oder sehr ähnlich. Damit ignoriert das Verfahren bei der Identifikation einer Bild- oder Videodatei mögliche Veränderungen der Größe, des Rauschfaktors, des Dateiformats oder eine Spiegelung des Bildes und konzentriert sich auf optische Übereinstimmungen. Die Wissenschaftler am Fraunhofer SIT haben diese Technik in einer Eigenentwicklung so verbessert, dass ein robuster Hash sogar das Beschneiden von Bildern übersteht: Ein Bild wird in Teilsegmente zerlegt und für jedes Segment wird ein Hash gebildet. Stimmen diese Teilsegment-Hashes beim Dateiabgleich überein, werden so selbst Ausschnitte bekannter Bilder gefunden.

Die robusten Hashes für zu untersuchende Bilder und beispielsweise auch Filme müssen sehr schnell zu berechnen und mit den in der Datenbank hinterlegten bekannten Hashes abzugleichen sein, damit große Mengen von Dateien möglichst zügig mit großen Datenbanken verglichen werden können. Das Verfahren des Fraunhofer SIT war von Anfang an mit Blick auf eine hohe Effizienz konzipiert, sodass die Hashberechnung schneller als bei konkurrierenden Verfahren durchgeführt werden kann.

Das Fraunhofer SIT hat nun zusätzlich die Abgleichgeschwindigkeit deutlich verbessert. Die Hash-Datenbank wird nicht linear durchsucht, sondern mittels spezieller Indexstrukturen, sodass pro Hash nicht die komplette Datenbank durchforstet werden muss, sondern nur ein Teilbereich. Damit sparen Ermittlungsbehörden viel Zeit und Ressourcen.

Eine zusätzliche Zeitersparnis bietet das sogenannte Stream-Carving. Um etwa eine beschlagnahmte Festplatte IT-forensisch zu untersuchen, wird zunächst eine IT-forensische Kopie der Platte erzeugt. Um Zeit zu sparen, nutzen die Experten des Fraunhofer SIT den Kopiervorgang für eine Vorabanalyse des Materials. Mit Stream-Carving wird der Datenstrom während des Kopierens bereits untersucht und auffällige Bilder und Videos werden erkannt.



Die robusten Hashs dieser Bilder unterscheiden sich in nur fünf Bits. Das Verfahren zeigt deshalb an, dass diese Bilder identisch sind.

Unser Angebot:

- Stream-Carving zur Vorabanalyse während der Datenakquisition
- IT-forensische Untersuchung von Videomaterial
- Identifizierung von veränderten Bilddateien, selbst nach Cropping
- Unterstützung sämtlicher gebräuchlicher Bildformate wie JPEG, PNG, GIF, BMP, TIFF
- Verfügbar für Microsoft Windows und Linux
- Image Hashing Tool mit grafischer Benutzeroberfläche (GUI)
- Image Hashing Tool für die Kommandozeile (CLI)
- Image Hashing SDK für C/C++ und Java
- Plugin für X-Ways Forensics
- Kostenlose Demo-Version

2.Platz 2012
Deutscher
IT-Sicherheitspreis

ForBild, das Vorgängerprojekt von ForSicht, wurde 2012 mit dem IT-Sicherheitspreis ausgezeichnet.