

Sehen im Dunklen

Wärmebildkameras im Kommen, 3D-Technik am Horizont: Das Simedia-Forum „Videoüberwachung/Videotechnik“ hat neue technische Möglichkeiten aufgezeigt.

Wie nehmen Computer Bewegung wahr? Antworten auf diese Frage gab DI Bernhard Strobl vom *Austrian Institute of Technology (AIT)* beim *Simedia-Jahresforum „Videoüberwachung/Videotechnik“*, das am 12. und 13. April 2011 in München stattgefunden hat.

Werden zwei Bilder miteinander verglichen und es ergeben sich beim zweiten Bild Veränderungen die leicht herausgerechnet werden können, kann das auf eine mittlerweile erfolgte Bewegung eines Objekts im Blickfeld rückführbar sein. Allerdings führen dann auch Bewegungen von Bäumen und Blättern im Wind, Lichtreflexionen und sogar das technisch bedingte Bildrauschen zu Fehldetektionen.

Es geht vielmehr darum, zusammenhängende Regionen als Objekt zu erkennen, einen „Blob“ zu errechnen, der in weiterer Folge nach der Bewegungsrichtung verfolgt und nach bestimmten Kriterien (Größe) gefiltert werden kann.

Das erfordert hohen Rechenaufwand und eine komplexe Parametrierung. Vom aufgenommenen Bildinhalt wird ein Bild errechnet, aus dem alle schnellen Bewegungen weggefiltert werden und das in Folge als Referenz für durch Objekte hervorgerufene Veränderungen herangezogen wird. Dieses Backgroundmodell muss etwa alle 30 Sekunden wechselnden Lichtverhältnissen (Sonne, Wolken, Tag/Nacht) angepasst werden.

Man kann in weiterer Folge Filter für die wahrzunehmenden Objekte entwickeln, nach Breite, Höhe, Fläche, Geschwindigkeit; Flächen,



Videoüberwachung: In Österreich ist die Videoüberwachung im neu eingefügten Abschnitt 9a des Datenschutzgesetzes erfasst.

die entweder ausgeblendet werden oder deren Überschreiten ein Alarmkriterium ist, oder eben eine richtungsabhängige Detektion. Realisiert wird dies über Regeln, die über einen Regeleditor dem System vermittelt werden.

Für Gesichts- und Personenerkennung werden Schablonen errechnet. In Entwicklung sind Suchstrategien mit Hilfe eines Avatars, einer virtuellen Gestalt, die einer in Bildsequenzen zu suchen Person (etwa eines Bankräubers) in Größe, Statur, bis hin zur Bekleidung, so weit als möglich angepasst werden kann. Im „Matching“ werden ähnliche Fundstellen ermittelt, die als Basis für weitere Überprüfungen dienen können.

Verhaltenserkennung.

Mehr als zwei Drittel der Bankräuber halten sich erfahrungsgemäß zur Informationsbeschaffung und/oder zum Abwarten eines geeigneten Zeitpunkts entweder im oder vor dem Geldinstitut auf. Im Rahmen des vom

österreichischen Sicherheitsforschungsprogramms *KIRAS* unterstützten Projekts „tribeB ID“ (Identifikation von Bedrohungsszenarien in Banken durch Bildanalyse) wurde nach Möglichkeiten gesucht, anormales und auffälliges Verhalten automatisch zu erkennen, mit dem Ziel, durch rechtzeitiges Erkennen eventueller Vorbereitungshandlungen Delikte zu verhindern.

Dr. Martin Kappel (TU Wien, Computer Vision Lab) berichtete über die Ergebnisse dieses im Februar 2011 abgeschlossenen Projekts. Ausgangspunkt war die Beobachtung des „normalen“ Verhaltens in Bankfilialen, etwa, wie lange sich eine Person im Foyer einer Bank oder bei einem Bankomaten aufhält. In 75 Prozent der Fälle war diese Zeitspanne unter vier Minuten. In der Verhaltensanalyse wurden viele atypische Fälle beobachtet, etwa Begleitpersonen, die gewartet hatten, spielende Kinder, mitgeführte Tiere, Reinigungs- und Sicherheitspersonal. Sonnenbrillen und

Kopfbedeckungen sind von der Jahreszeit abhängig. Als Hauptschwierigkeiten haben sich Verdeckungen herausgestellt, nicht nur wegen nicht eingesehener Bereiche, sondern weil bei Einsatz von nur einer Kamera bei zwei Personen, die einander entgegenkommen und sich dann optisch überdecken, bei der automatischen Bildanalyse nicht gesagt werden kann, ob sich die beiden jeweils in ihrer Richtung weiterbewegen oder wieder zurückgehen. Komplexe Hintergründe, schnelle Bildänderungen, Reflektionen, Schatten, bereiten ebenfalls Probleme.

Es hat sich als nicht ausreichend herausgestellt, sich auf automatisiert festgestellte Abweichungen vom Normverhalten zu konzentrieren. Die automatisierte Verhaltenserkennung Sinn: Sie erfordert keine neue, zusätzliche Überwachung, sondern nützt das bestehende Videosystem besser aus. Im automatisiert ermittelten Verdachtsfall kann, ohne dass gleich Alarm ausgelöst oder jemand als „Verdächtiger“ geführt würde, bei Verwendung hochauflösender Kameras auf eine bessere Bildqualität (High Resolution), mit Speicherung von Gesichtsbildern in hoher Qualität, umgeschaltet werden, da dies im Dauerbetrieb wegen des zu großen Speicherbedarfs unwirtschaftlich wäre. Sollte es tatsächlich zu einem Raubüberfall kommen, liegen fahndungsrelevante Informationen rasch vor, weil Aufnahmen von derartigen Verdachtsfällen schneller durchsucht werden können. Mit kalibrierten Kamerasystemen kann durch manuelles Klicken auf Fuß- und Kopf-



„Reeperbahn“ in Hamburg: Öffentliche Bereiche können mit Videokameras überwacht werden.



Wärmebildkameras liefern auch bei leichtem Nebel, Regen oder Rauch klare Videobilder.

punkt automatisch die Größe der Zielperson errechnet werden. Gegebenenfalls zu hinterfragende Verdachtsfälle sind auch eine unübliche Verweildauer im Foyer außerhalb der Öffnungszeiten oder an Bankomaten. Manipulationen an Geldausgabeautomaten dauern wesentlich länger als Geldbehebungen durch Kunden.

Nachdem Mitarbeiter in der Regel nur bedingt die Möglichkeit haben, ihr Arbeitsumfeld zu beobachten, gibt das System Hinweise und lenkt die Aufmerksamkeit auf ein Geschehen, ohne Fehlalarme zu produzieren. Es obliegt dann dem Sicherheitspersonal oder den Mitarbeitern, die Situation zu beobachten und zu verifizieren, etwa durch Ansprechen der Person („Kann ich Ihnen helfen?“). Ein potenzieller Täter wird sich beobachtet fühlen und dadurch möglicherweise abgehalten, einen Überfall zu begehen.

Bei Banken geht der Trend dahin, möglichst viel von den Kassen im Kundenfoyer in den Selbstbedienungsbereich zu verlagern. Nach wie vor liege der Schwerpunkt der Videoüberwachung aber im Kassensbereich, und damit bei den klassischen Kriminalitätsformen wie Raubüberfall, Geiselnahme und Einbruch, erläuterte Gerhard

Reinhardt, Leiter Sicherheit der *Commerzbank AG*.

Die Kriminalität habe sich aber eher in den SB-Bereich verlagert, wo sich Formen der Kriminalität wie Skimming, Aufbrechen von Hartgeldeinzahlungsmodulen, Aufbrüche oder Sprengungen von Geldautomaten, Überweisungs- und Abhebebetrug, Cash-Trapping und Vandalismus entwickelt haben. Beim Cash-Trapping wird das auszubehende Bargeld an Klebestreifen zurückgehalten. Auf die geänderten Tatabläufe werde bei der Videoüberwachung noch zu wenig eingegangen, obwohl gerade hier beispielsweise beim Aufbrechen oder Sprengen von Geldausgabeautomaten die Schäden größer seien als etwa bei Raubüberfällen, betonte Reinhardt. Der Einsatz von Videotechnik liefere einen Mehrwert, nämlich durch Erstellung eines Täterprofils, durch Schaffung von Beweismitteln und bei der Reduktion der Schadensregulierungskosten. Videoüberwachung decke die meisten kriminellen Handlungen im Bankenbereich ab; Bewegungsmelder, Magnetkontakte, Überfallmelder, Einbruchsmeldeanlagen hingegen nur jeweils einen Teilbereich. Reinhardt: „Videotechnik ist künftig eine der Kernkomponenten der Sicherheitstechnik.“

Mit der 3D-Technik begibt man sich in der Videoüberwachung auf Neuland. Albrecht Gasteiner vom *HDTV-Forum Schweiz* (www.hdtv-forum.ch) erläuterte die Möglichkeiten der technischen Realisierung des räumlichen Sehens im digitalen Umfeld.

Grundsätzlich müssen die Bildinformationen für das linke und das rechte Auge getrennt aufgenommen und ebenfalls getrennt wiedergegeben werden, damit beim Betrachter der räumliche Eindruck entstehen kann.

Veraltet ist das Anaglyphen-Verfahren, das eine Rot-Grün-Brille erfordert. Die Bildqualität ist schlecht. Mit dem 2D ist das Verfahren nicht kompatibel, da der Rot- und Grünanteil des Bildes zueinander versetzt zugeleich sichtbar sind.

Bei dem am weitesten verbreiteten „Frame-Sequential-Prinzip“ werden in der Zeit, in der normalerweise ein Vollbild wiedergegeben wird (1/25 sec), auf einem schnellen Bildschirm zwei Vollbilder nacheinander dargestellt, nämlich jeweils das für das linke und das rechte Auge. Eine „Shutter-Brille“ sorgt durch synchron ablaufendes Abdecken des linken und des rechten Auges dafür, dass jedes Auge den passenden Bildinhalt erhält.

Das Abdecken erfolgt durch LCDs, die im Takt des

Bildwechsels abwechselnd durchlässig/nicht durchlässig geschaltet werden. Die Synchronisierung zum Fernsehbild wird über einen Infrarotempfänger hergestellt. Der Betrachter kann sich vor dem Bildschirm frei bewegen. Zudem bietet das Verfahren höchste Bildqualität. Nachteile sind der Preis und das Gewicht der Brille.

Beim Polarisationsverfahren werden die beiden Bildinformationen gleichzeitig wiedergegeben, und zwar der eine Bildstrom auf den geradzahligen Zeilen des Bildschirms, der andere auf den ungeradzahligen („interlaced“). Ein vor dem Bildschirm angebrachter Filter polarisiert das Licht von den geradzahligen Zeilen anders als das von den ungeradzahligen.

Über eine leichte und preisgünstige Polarisationsbrille erhält jedes Auge die passende Information. Die Auflösung ist insofern geringer, als jedes Auge nur die Hälfte des Bildinhalts erhält.

Eine Aufteilung des Bildinhalts erfolgt auch bei autostereoskopischen Bildschirmen, bei denen für das räumliche Sehen keine Brille benötigt wird.

Ein vor dem Bildschirm angebrachtes System feiner Mikrolinsen lenkt die jeweilige Bildinformation auf einen Punkt in einem definierten Abstand. Befindet man



Referenten beim Jahresforum „Videoüberwachung/Videotechnik“: Martin Huff, Bernhard Strobl, Martin Kampl, Peter Loibl.

sich mit den Augen dort, entsteht ein räumliches Bild, aber nur in diesem engen Bereich. Für einen Wohnraum ist das ein Problem, kaum jedoch für einen Betrachter vor dem Bildschirm einer Leitstelle.

3D-Bilder werden üblicherweise von zwei Kameras im Augenabstand von 6,5 cm aufgenommen, wobei die Kameras möglichst gleich eingestellt sein müssen. Um eine größere räumliche Tiefe zu erreichen, kann der Abstand vergrößert werden.

Für Transport, Speicherung und Bearbeitung von 3D-Informationen hat sich bei den europäischen Fernsehanstalten mittlerweile ein Verfahren eingebürgert, bei dem die beiden Bildinformationen jeweils auf die Hälfte ihrer Breite zusammengedrückt werden und damit auf ein normales 16:9-Bild passen. 3D-geeignete Bildschirme erkennen das und entzerren die Bilder wieder.

Überall dort, wo Bedarf besteht, flächige Bilder in die Tiefe aufzulösen, können sich Anwendungen der 3D-Technik ergeben. Das bereits beschriebene Problem bei der Richtungsverfolgung entgegenkommender Objekte ließe sich damit lösen, oder auch die Frage, wer in einer Menschenansammlung (Stadion) was getan hat.

Herkömmliche fotografische Techniken lassen bei der flächenhaften Darstellung mitunter eine eindeutige Zuordnung nicht zu. Die Entwicklung steht erst am Anfang.

Wärmebildkameras für Videodetektionssysteme sind im Kommen. Ihr Erfassungsbereich geht bis etwa 500 Meter und erreicht damit etwa das Vierfache herkömmlicher Videokameras. Sie sind, da sie auf Wärmestrahlung ansprechen, von Lichtquellen unabhängig und somit bei Tag und Nacht sowie bei schlechten Sichtverhältnissen (Regen, Nebel) einsetzbar. Datenschutzrechtlich ist bemerkenswert, dass eine Personerkennung wegen fehlender Detaillierung der Bilder nicht möglich ist, also keine personenbezogenen Daten verarbeitet oder gespeichert werden. Menschen werden bloß detektiert, aber nicht identifiziert. Die Verifikation eines detektierten Vorgangs muss in der Folge über herkömmliche Videokameras erfolgen.

Datenschutz. Über Rechtsfragen, die sich im Zusammenhang mit der Videoüberwachung in Deutschland ergeben haben, berichtete Rechtsanwalt Martin W. Huff. Die Beobachtung öffentlich zugänglicher Räume

mit optisch-elektronischen Einrichtungen ist in § 6b des Bundesdatenschutzgesetzes (BDSG) geregelt, die Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses in § 32 BDSG.

Für den österreichischen Rechtsbereich ist die Videoüberwachung seit der am 1. Jänner 2010 in Kraft getretenen DSGVO-Novelle 2010 (BGBl I 2009/ 133) im neu eingefügten Abschnitt 9a des DSGVO erfasst (siehe *Öffentliche Sicherheit*, Nr. 5-6/10, S. 93 – 97).

Als „öffentlich zugängliche Räume“ werden Gebäude, Tiefgaragen, Kaufhäuser, Banken, Büros usw. angesehen, sowie Räume und umgrenzte Bereiche, die ohne oder nur mit einer schematischen Kontrolle (EC-Karte) für einen unbestimmten Personenkreis zugänglich sind. Gegen den Einsatz der Videotechnik im öffentlichen Bereich haben die Gerichte in Deutschland bisher in der Regel keine rechtlichen Bedenken geäußert. So wurde durch das OVG Hamburg mit Urteil vom 22.6.2010, 4 Bf 276/07, die Überwachung öffentlicher Teile der Hamburger Reeperbahn (nicht der Hauseingänge) für zulässig erklärt, ebenso die Überwachung von Geldautomaten, des Eingangs von Kaufhäusern und der Einfahrt von

Tiefgaragen und Eingangshallen. Wie in Österreich muss in Deutschland der Betriebsrat einer offenen Überwachung in einem Unternehmen zustimmen. Im öffentlich zugänglichen Bereich ist auch die dauernde Überwachung erlaubt (Bahnhöfe, Kassenbereiche von Banken, Spielbanken; Personennahverkehr).

Als zulässig angesehen wurde die Überwachung einer Schwimmhalle und der Schränke, nicht aber der Umkleide- und Nacktbereiche; in einem Kaffeehaus die Überwachung des Kassen- und Warenbereichs, nicht aber des Kundenbereichs.

Probleme haben sich ergeben bei der Überwachung der Bibliothek einer Hochschule (OVG Münster, 8.5.2009, 16 A 3375/07; keine Speicherung der Daten), oder beim Einsatz an Tankstellen – ein zivilrechtlicher Auskunftsanspruch gegenüber dem ermittelten Halter wurde verneint. Eine verdeckte Überwachung ist nur in Ausnahmefällen zulässig.

Eine Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen ist nach § 201a dStGB strafbar. Eine vergleichbare strafrechtliche Regelung fehlt für den österreichischen Rechtsbereich.

Kurt Hickisch