Croce-Ferri, Steinebach, Knoth; Praxisnaher koalitionssicherer Fingerabdruckalgorithmus für Bilder, Tagungsband D-A-CH Security 2006, Horster (Hrsg.), syssec Verlag, ISBN 3-00-018166-0, S. 236-247, 2006

Praxisnaher koalitionssicherer Fingerabdruckalgorithmus für Bilder

Lucilla Croce Ferri, Martin Steinebach, Mia Knoth

Fraunhofer Institut Integrierte Publikations- und Informationssysteme
Dolivostraße 15; 64293 Darmstadt
(lucilla.croce-ferri, martin.steinebach)@ipsi.fraunhofer.de

Zusammenfassung

Das Internet ist ein effizienter Weg, digitale Medien sowohl legal als auch illegal zu verbreiten. Mittels digitaler Wasserzeichen kann zumindest die Quelle einer illegalen Weitergabe identifiziert werden, wenn individuelle Kundenmerkmale in die Medien eingebettet werden. Um dabei vor einer Reihe bekannter Angriffe gegen die eingebetteten Kundenmerkmale sicher zu sein, werden koalitionssichere digitale Fingerabdrücke eingebettet. Derzeit führt die Verwendung von aktiven Fingerabdrücken bei steigender Kundenzahl schnell zu enormen Anforderungen hinsichtlich der Kapazität digitaler Wasserzeichen. Wir stellen ein Konzept vor, mit dem anhand der Kenntnis über potentielle Verbreitungswege ein effizientes Erstellen von Kundenmerkmalen möglich ist.

Motivation

Durch die Ausweitung des Internets und die dadurch steigende Teilnehmerzahl entsteht ein immer größer werdender digitaler Marktplatz. Da auch die Breitbandnetzwerke eine fortwährende Entwicklung erfahren, wird eine stets ansteigende Menge von Multimediadaten durch das Netzwerk verteilt.
Hierbei ist allerdings nicht nur die Möglichkeit gegeben, die Daten zu verteilen, sondern es ergibt sich auch das Problem, sicherzustellen, dass diese Daten vom Empfänger dann auch auf angemessene Weise verwendet werden. Deshalb ist ein Schutz vor unrechtmäßigem Gebrauch und Verteilung von Multimediadaten dringend notwendig. In das Datenmaterial eingebrachte Markierungen, die als digitale Wasserzeichen bezeichnet werden, können hier helfen, diesen Schutz zu bieten.
Die digitalen Wasserzeichen finden in vielen verschiedenen Bereichen ihre Anwendung. Eine davon ist auf dem Einsatz digitaler Fingerabdrücke basiert. Das ermöglicht die Kontrolle der Verteilung von Daten und das Aufspüren von Kunden, die ihre legal erworbenen Daten für unberechtigte Zwecke gebrauchen. Die kundenspezifischen Abdrücke werden von dem Verkäufer in die Daten eingebracht, bevor er sie an seine Kunden verteilt. Eine einfache und effektive Methode gegen die digitalen Fingerabdrücke vorzugehen, stellt die Methode dar, dass sich die Kunden zu einer Koalition zusammenschließen, in der mehrere verschieden markierte Kopien der gleichen Originaldaten kombiniert werden, um den unterliegenden Fingerabdruck abzuändern. Dieses Vorgehen wird als Koalitionsattacke bezeichnet. Digitale Fingerabdrücke sollten deshalb nicht nur robust gegen allgemeine Datenbearbeitungsangriffe sein, wie herkömmliche Wasserzeichenverfahren, sondern auch gegen Koalitionsattacken.
In der Literatur wird teilweise zwischen passiven und aktiven Fingerabdrücken unterschieden. Unter passiven Fingerabdrücken versteht man Vektormerkmale, die aus digitalen Inhalten extrahiert werden und die den Inhalt eindeutlich charakterisieren können. Sie können zur Inhaltsidentifizierung eingesetzt oder als Wasserzeichen zur Überprüfung der Datenintegrität eingebettet werden. In der engli-

schen Literatur werden solche Verfahren mit verschiedenen Begriffen benannt: robust hashing, perceptual hashing, passive fingerprinting, robust signatures. Um für multimediale Anwendungen geeignet zu sein, müssen die extrahierten inhaltsabhängigen Merkmale robust gegenüber Datenbearbeitungsoperationen [CBK02] sein. Die hier besprochene Technologie ist dagegen ein aktives Verfahren. Darunter versteht man eine spezielle Anwendung von digitalen Wasserzeichen, mit der man Informationen zur Kundeidentifizierung in den Daten einbettet. Dadurch unterscheiden sich die markierten Datenversionen leicht voneinander und eröffnen Angriffsmöglichkeiten, wie die Koalitionsattacke, die nur bei dieser Wasserzeichenanwendung vorkommen können.

Ziel dieses Beitrages ist, die Einsatzgebiete koalitionssicherer Fingerabdruckalgorithmen für Bilder anhand verschiedener Szenarien zu erläutern und einen Algorithmus darzustellen, dessen Effizienz bei der Detektion durch soziale Kenntnisse der Kundschaft gesteigert werden kann.

1 Einfache mögliche Angriffe

Bei der kundenspezifischen Markierung eines Medium mit digitalen Fingerabdrücken entstehen mehrerer Kopien, welche sich leicht voneinander unterscheiden. Ist ein potentieller Angreifer nur im Besitz einer dieser markierten Kopien so kann er die Fingerabdruckinformation, ohne Kenntnis des verwendeten Einbettungsalgorithmus und des entsprechenden geheimen Schlüssels nicht detektieren.

Vergleichen jedoch mehrere Eigentümer legaler Kopien ihr Datenmaterial, können sie die Unterschiede auffinden. Diese Gegenüberstellung der Kundenkopien erfolgt pixelweise. Man spricht hier von einem Koalitions- oder Vergleichsangriff (engl.: „collusion attack“). Ist das Verfahren nicht robust gegen den Angriff, kann dabei eine neue Kopie entstehen, die entweder kein detektierbares Wasserzeichen mehr enthält oder aber eines, welches einen unschuldigen Kunden identifiziert.

Es gibt mehrere Formen von Koalitionsangriffen, abhängig von der Methode, wie sie durchgeführt werden. Wirkungsvolle Attacken lassen sich schon mit gängigen Bildbearbeitungsprogrammen einfach durchführen, indem man z.B. mehrere Bilder überlagert (Durchschnittsattacke: siehe **Abb. 1**). Je mehr Angreifer an dieser Attacke beteiligt sind, desto geringer ist die Wahrscheinlichkeit den einzelnen Kunden zu verfolgen, da bei einer großen Anzahl von Mitwirkenden der Anteil jedes individuellen Fingerabdruckes für die Durchschnittbildung gering ist.

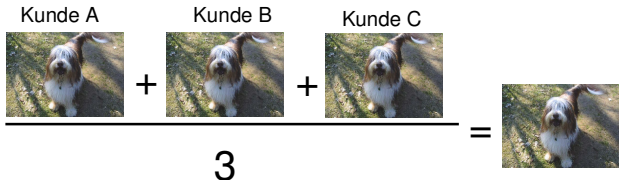


Abb. 1: Durchschnittattacke

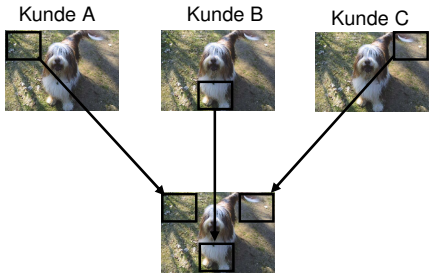


Abb. 2: Mosaic-Attacke

Eine neue Version der Kopien kann auch generiert werden, indem pixelweise die Maximal/Minimalwerte zweier mit unterschiedlichen Fingerabdrücken markierten Bilder übernommen werden.

Ein weiteres Beispiel für Koalitionsattacken ist die Mosaic-Attacke. Die an „Mosaic-Attacke“ (**Abb. 2**) beteiligten Kunden schneiden jeweils Teile aus ihrem markierten Datenmaterial aus und fügen danach erneut diese Teile zusammen, um ein verändertes Fingerabdrucksignal zu erhalten.

2 Digitale Fingerabdruckalgorithmen

Der Einbettungsprozess des digitalen Fingerabdruckes lässt sich in drei Teilprozesse wie folgt gliedern: a) Erzeugung des Fingerabdruckes, b) Ermittlung der Markierungspositionen, c) Einbettung des Fingerabdruckes.

Auch der Ausleseprozess des digitalen Fingerabdruckes lässt sich in drei Teilschritte gliedern: a) Erzeugen der Markierungspositionen, b) Abfrage des Fingerabdruckes, c) Analyse des ausgelesenen Fingerabdruckes. Bei der Abfrage kann sich um eine nicht-blinde Detektion unter Zuhilfenahme des Originalbildes während des Detektionsvorganges oder um eine blinde Detektion handeln, bei der das Originalbild nicht zu Verfügen steht. Die Unterschiede zwischen dem blinden und dem nicht-blinden Verfahren werden in [StCr05] ausführlich diskutiert.

Die meisten Abfrageprozesse für eine nicht-blinde Detektion bauen auf Korrelationen auf. Dabei wird als Erstes der zu untersuchende Fingerabdruck gewonnen, indem das Original von der aufgefundenen Kopie subtrahiert wird. Hiernach wird die Ähnlichkeit zwischen dem extrahierten Fingerabdruck und jedem einzelnen originalen Fingerabdruck geprüft und als Ergebnis der Detektion kann auf die zuvor eingebetteten Fingerabdrücke geschlossen werden.

2.1 Spezielle Anforderungen

Algorithmen zum Einbetten digitaler Fingerabdrücke sind ein Sonderfall digitaler Wasserzeichen zum Schutz von Urheberrechten. Deswegen lassen sich gemeinsame Anforderungen feststellen. Eine der wichtigsten davon ist eine **fehlende Wahrnehmbarkeit** der eingebetteten Fingerabdrücke, da die Qualität der markierten Bilder nicht durch die Markierung reduziert werden darf. **Robustheit** ist ebenso wichtig, da alle bei digitalen Wasserzeichen denkbaren Angriffe ebenfalls auf digitale Fingerabdrücke übertragbar sind. Die Fingerabdrücke müssen auch robust in die Daten eingebettet werden, damit sie sowohl gezielten als auch zufälligen Veränderungen des Datenmaterials standhalten. Hingegen handelt es sich bei der am häufigsten vorkommenden Attacke auf digitale Fingerabdrücke, dem Koalitionsangriff, um eine Angriff, der nur auf digitale Fingerabdrücke zielt, da diese Attacke lediglich durch das Verteilen unterschiedlicher Kopien des Datenmaterials ermöglicht wird. Ziel eines Koalitionsangriffes ist das Entfernen des Fingerabdrucks bzw. das Bilden eines neuen oder einem anderen Käufer zugeordneten Fingerabdrucks.

Koalitionssichere Fingerabdruckalgorithmen müssen so gestaltet sein, dass die Chance, mindestens einen Angreifer zu identifizieren, maximiert wird. Gleichzeit muss die Wahrscheinlichkeit, einen unschuldigen Kunden fälschlich zu beschuldigen, minimiert werden. Ein Detektionsansatz schlägt fehl, wenn es dem Detektor entweder misslingt, einen der Schuldigen zu identifizieren oder wenn er einen unschuldigen Kunden als schuldig bezeichnet. Dieses Kriterium spielt speziell vor Gericht eine bedeutende Rolle.

Die Eigenschaft eines Verfahrens, gegen Koalitionsangriffe robust zu sein, wird **Kollusionsresistenz** genannt. Die Anzahl der für einen erfolgreichen Koalitionsangriff notwendigen Kopien gibt die Kollusionsresistenz eines Verfahrens an.

Eine **niedrige Komplexität** und eine hohe Einbettungsgeschwindigkeit sind noch zusätzliche spezielle Anforderungen an Fingerabdruckalgorithmen, da sonst der Aufwand für das Einbetten verschiedener Fingerabdrücke erheblich steigen kann. Das Verwenden des Originalbildes bei einer nicht-blinden Detektion ist hilfreich, um die Synchronisierung des Wasserzeichens nach möglichen Angriffen zu ermöglichen und dadurch die Robustheit des Verfahrens zu erhöhen. Wenn also das Einsatzszenario ein nicht-blindes Verfahren erlaubt, ist dieses bevorzugt einzusetzen.

Die **Kapazität** des Verfahrens beschreibt die Menge der Information, die ohne Verlust von Transparenz und Robustheit eingebettet werden kann. Sie muss möglicht hoch sein, um genug Raum für die datenintensiven Fingerabdrücke zu lassen. Deren tatsächliche Länge ist von der Anzahl der Kunden und vermuteten Piraten sowie vom gewählten Algorithmus abhängig.

2.2 Bekannte Ansätze

Es gibt mehrere unterschiedliche Ansätze, um koalitionssichere digitale Fingerabdrücke zu erreichen. Das Ziel der existierenden Ansätze liegt nicht darin, Koalitionsangriffe zu verhindern, sondern nach einer solchen Attacke die schuldigen Raubkopierer zu identifizieren.

Eine wichtige Gruppe von koalitionssicheren Fingerabdrücken sind die **nicht-codierten Fingerabdrücke**, auch **orthogonale Fingerabdrücke** genannt: Bei den orthogonalen Fingerabdrücken handelt es sich um die ersten entwickelten Fingerabdrücke, die eine gute Robustheit gegen Koalitionsattacken aufwiesen [BoSh98]. Fingerabdrücke stellen Vektoren unterschiedlicher Länge dar, deren Elemente 1 oder 0 sind. In diesem Sinn versteht man in der Praxis unter orthogonale Fingerabdrücke Vektoren, die pseudozufällig generiert wurden, deren Elemente eine sehr niedrige Korrelation miteinander zeigen.

Die Eigenschaft dieser Gruppe ist, dass die digitalen Fingerabdrücke der einzelnen Kunden orthogonal zueinander aufgebaut sind. Orthogonale Fingerabdrücke haben die positiven Eigenschaften, dass sie einfach herzustellen und in das Datenmaterial einzubetten sind. Ein großes Problem der orthogonalen Fingerabdrücke ist, dass die Anzahl der benötigten Fingerabdrücke linear mit der Anzahl der Kunden steigt. Auch die Komplexität der Detektion der orthogonalen Fingerabdrücke steigt linear mit der Kundenzahl. Da jeder einzelne originale eingebettete Fingerabdruck mit dem aufgefundenen zu testenden Fingerabdruck korrelieren muss, ergibt sich eine Anzahl von Vergleichen, die proportional zu den Kunden ist. Daraus ergibt sich bei einer großen Kundengruppe eine entsprechend aufwendige und langwierige Detektion.

Neben den nicht-codierten Fingerabdrücken existiert noch eine andere bedeutende Gruppe der koalitionssicheren Fingerabdrücke, nämlich die **codierten Fingerabdrücke**. Die Idee der codierten Fingerabdrücke beruht auf dem Gedanken, dass die Piraten bei einem Vergleich ihrer Kopien nur die Unterschiede ihrer Fingerabdruckvektoren auffinden und manipulieren können, die identischen Informationen sind jedoch nicht auffindbar. Deshalb müssen die Fingerabdruckvektoren so gestaltet sein, dass genügend Restinformationen in den identischen Teilen der Vektoren liegen, um die an der Koalition beteiligten Kopien und somit die Piraten zu identifizieren. Ein großer Vorteil der codierten gegenüber den orthogonalen Fingerabdrücken ist, dass durch die Beziehungen der einzelnen Fingerabdruckvektoren zueinander wesentlich weniger Basissignale als bei den orthogonalen Fingerabdrücken benötigt werden. [WTWL04]. Basissignale sind Signale, durch deren gewichtete Summe alle anderen Fingerabdrücke generiert werden. Nachteilig für die Verwendung codierter Fingerabdrücke erweist sich die Tatsache, dass die obere Grenze der Anzahl der Angreifer im Falle einer Koalition schon während der Fingerabdrücke für ein bestimmtes Höchstmaß an Angreifern, die miteinander koalieren, festgelegt werden muss. Schließen sich jedoch mehr Piraten zu einer Koalition zusammen als während der Konstruktion der codierten Fingerabdrücke vorgesehen war, so können diese Angreifer nicht identifiziert werden.

Bei den codierten Fingerabdrücken basiert eine Gruppe auf die Theorie der Kombinatorik. Diese koalitionssicheren Fingerabdrücke werden Anti-Koalitionscodes (ACC) genannt [TWWL03]. ACC Fingerabdrücke sind so definiert, dass beliebige bitweise Kombinationen durch z.B. eine UND-Verknüpfung der Fingerabdrücke keine Repetition derselben Ergebnisse produzieren. Eine exaktere mathematische Definition kann in [TWWL03] gefunden werden.

Ein Ansatz, der sowohl die Eigenschaften von uncodierten digitalen Fingerabdrücken als auch von codierten Fingerabdrücken verbindet, ist der **Cluster-Ansatz** [WWTL04] [HeWu05]. Er basiert auf der Annahme, dass die Piraten bzw. Kunden mit illegalen Absichten sich mit bestimmten Kreisen bevorzugt zusammenschließen. Dieser Zusammenschluss der Piraten hängt mit sozialen, kulturellen, geographischen und anderen Gemeinsamkeiten zusammen. Die Kunden, die untereinander Gemeinsamkeiten aufweisen, werden zu einer Gruppe – auch Cluster genannt – zusammengefasst. Es entstehen so verschiedene Gruppen, wobei die Kunden von unterschiedlichen Cluster jedoch keine Gemeinsamkeiten besitzen. Somit ist eine intra-Gruppe Koalition viel wahrscheinlicher als eine inter-Gruppe Koalition. Die Fingerabdrücke müssen also so gestaltet sein, dass die Fingerabdrücke einer Gruppe orthogonal zu denen einer anderen Gruppe sind. Im Gegensatz dazu müssen die Fingerabdrücke innerhalb eines Clusters weitgehend Übereinstimmungen aufweisen. Um Fingerabdrücke zu konstruieren, die Gemeinsamkeiten und Unterschiede zwischen den einzelnen Kunden berücksichtigen, werden als Übersicht über die Eigenschaften der Kunden Organigramme erstellt.

Wenn eine Kopie mit einem veränderten Fingerabdruck entdeckt wird, wird als Erstes das betreffende Cluster identifiziert und anschließend muss innerhalb dieses identifizierten Clusters nach den Schuldigen gesucht werden.

3 Darstellung des eigenes Verfahrens

Das in diesem Beitrag dargestellte Verfahren ist durch die Verknüpfung und Optimierung teilweise schon existierender Ansätze entstanden. Ziel unserer Arbeit war die Entwicklung eines Algorithmus, der die Vorteile verschiedener in der Literatur vorgestellter Ideen kombiniert dessen Aufwand bei der Implementierung und Durchführung praxistauglich ist.

Die Erfahrung, die wir durch industriebezogene Projekte gesammelt haben, zeigt, dass der Auftraggeber für die Entwicklung eines Fingerabdruckverfahrens oft daran interessiert ist, einen schon existierenden Verdacht zu konkretisieren. Darauf basierend, sollen bestimmte Verbreitungswege der Daten in der Zukunft vermeidet werden. Dabei spielt die Kenntnisse über die Kunden und deren Einwirkungskreis eine wichtige Rolle.

Aus diesem Grund verspricht der Cluster-Ansatz einige Vorteile. Der Zweck der Cluster-Bildung ist, Kunden mit gleichen Interessen innerhalb einer Gruppe mit ähnlichen Fingerabdrücken zu versehen. Da die Anti-Koalitionscodes den Sinn haben, ähnliche Fingerabdrücke zu generieren, eignet sich die Verknüpfung der Gruppenidee mit den Anti-Koalitionscodes. Das eingesetzte Wasserzeichen besteht somit aus zwei Teilen:

1. Der erste Teil des eingebetteten Wasserzeichens beinhaltet die Information, zu welcher Gruppe der Kunde gehört. In dem Verfahren bekommt deswegen jede Gruppe einen spezifischen Geheimschlüssel zugewiesen, der zur Generierung dieses Teiles eingesetzt wird.
2. Der zweite Teil des eingebetteten Wasserzeichens ist kundenspezifisch, wobei hier ACC Fingerabdrücke verwendet werden.

Tab. 1: Gegenüberstellung eines prinzipiellen und des entwickelten Fingerabdruckalgorithmus

Prinzipieller Fingerabdruckalgorithmus	**Entwickelter Fingerabdruckalgorithmus**
A) Einbettungsprozess	
A1) Ermitteln der Markierungspositionen	A0) Gruppenteilung der Kunden A1) Ermitteln der Markierungspositionen durch Differenzbildung von Originalbild und komprimierten Bild
A2) Generierung der Fingerabdrücke	A2) mittels Geheimschlüssel und ACC Fingerabdrücke werden Wasserzeichen erzeugt
A3) Einbettung der zuvor generierten Fingerabdrücke	A3) Einbettung der Wasserzeichen durch Verwenden des unter [DFHJ00] beschriebenen Algorithmus
B) Abfrageprozess	
B1) Ermitteln der Markierungspositionen	B1) siehe A1)
B2) Detektion der zuvor eingebetteten Fingerabdrücke	B2) Auslesen des eingebetteten Wasserzeichens B3) Detektion der Gruppe durch Korrelationsberechnung B4) Detektion der Fingerabdrücke innerhalb einer Gruppe durch Korrelationsberechnung

Um einen Überblick zu liefern, welche Teilschritte für den entwickelten Fingerabdruckalgorithmus notwendig sind, wird in der Tabelle 1 die schrittweise Abfolge eines Standard-Fingerabdruckalgorithmus mit dem entwickelten koalitionssicheren Fingerabdruckalgorithmus verglichen.

Die einzelnen Komponenten des Einbettungsprozesses werden im Folgenden erklärt:

A0) Gruppenteilung der Kunden: Mit von Anwendung abhängigen Kriterien werden bei diesem Schritt die Kunden in verschiedene Gruppen geteilt. Die Kriterien sollen so gewählt werden, dass die Wahrscheinlichkeit einer inter-Gruppe Attacke minimiert wird.

A1) Ermittlung der Markierungspositionen: Die Art und Weise wie die Markierungspositionen bestimmt werden und wie der Einbettungsprozess abläuft, wird teilweise von einem in [DFHJ00] beschriebenen Algorithmus übernommen. Es wird eine JPEG-Kompression des Originalbildes mit festem Kompressionsfaktor durchgeführt und die Differenz zwischen dem komprimierten Bild und dem Original gebildet. Die Pixel der zwei Bilder, die eine Wertdifferenz zeigen, werden als Positionen für das Einbetten des Wasserzeichens gewählt. Je niedriger der Kompressionsfaktor gewählt wird, desto mehr Markierungspositionen entstehen. Fällt die Wahl auf einen zu höherem Kompressionsfaktor, so kann dieses die Transparenz durch eine zu große Anzahl von Markierungspositionen negativ beeinflussen. Andererseits ist ein höherer Kompressionsfaktor für die Robustheit gegenüber späteren JPEG-Operationen von Vorteil. Komplexe Bilder, die eine hohe Anzahl von Konturen und verschiedenen Farbübergängen besitzen, enthalten auch viele Markierungspositionen, da die Differenz an vielen Stellen ungleich 0 ist. Alle Kundenkopien haben identische Markierungspositionen.

A2) Erzeugung des Wasserzeichens: Das Wasserzeichen ist ein binärer Vektor, deren Länge die Anzahl der Markierungspositionen gleicht. Seine Elemente werden durch eine bitweise XOR Verknüpfung von zwei Bit-Sequenzen festgelegt. Die erste Sequenz wird pseudozufällig in Abhängigkeit des Geheimschlüssels generiert, die zweite besteht aus der Widerholung eines ACC Fingerabdruckes. Für die Tests werden die 20 Fingerabdrücke von [Wu05] mit 16 bits verwendet, sodass 20 Kunden innerhalb einer Gruppe möglich sind.

A3) Einbettung der Wasserzeichen: Abhängig von den bits des Wasserzeichens wird die in Teilprozess A1) berechnete Differenz von den Pixeln des Originalbilds, die zur Markierungspositionen gehören, subtrahiert (bit=0), bzw. addiert (bit=1). Alle Pixel des Originales, die nicht als Markierungsposition durch das Teilprozess A1) identifiziert wurden, bleiben unverändert.

Die einzelnen Komponenten des Abfrageprozesses sind:

B1) Ermittlung der Markierungspositionen: Da die Markierungspositionen bestimmt werden sollen, in denen das Wasserzeichen eingebettet wurde, verläuft die Ermittlung dieser Positionen analog zum Einbettungsprozess A1). Schließlich müssen sich bei der Detektion dieselben Positionen wie bei der Einbettung ergeben. Auch der Kompressionsfaktor muss den gleichen Wert wie bei dem Einbettungsprozess besitzen, da sich sonst bei dem Abfrageprozess andere Markierungspositionen ergäben.

B2) Auslesen des eingebetteten Wasserzeichens: Bei diesem Teilprozess wird es rekonstruiert, ob der Pixelwert des markierten Bildes bei den jeweiligen Markierungspositionen vergrößert oder verkleinert wurde. Das geschieht in dem man die Differenz zwischen markier-

tem Bild and Original an der Stelle überprüft. Ist die Differenz positiv setzt man in der Bitsequenz des rekonstruierten Wasserzeichens eine 1, ist sie negativ, setzt man eine 0.

B3) Gruppenabfrage: Mit dieser Abfrage wird zuerst festgestellt, zu welcher Gruppe möglicherweise der eingebettete Fingerabdruck gehört. Eine pseudozufällige Sequenz in Abhängigkeit eines Geheimschlüssels wird generiert und direkt korreliert mit dem Wasserzeichen, das aus dem Teilprozess B3) rekonstruiert wurde. Gehört das Bild zur Gruppe mit dem Schlüssel, der gerade überprüft wird, hat man eine hohe Korrelation, sonst ist die Korrelation niedrig. (siehe **Abb. 3**(a)

B4) Fingerabdruckabfrage: Nachdem man die Gruppe identifiziert hat, wird der Fingerabdruck gesucht. Das in B2) ausgelesene Wasserzeichen wird zuerst mit einer XOR Operation mit allen 20 zur Verfügung stehenden Fingerabdrücken verknüpft. Das Ergebnis wird mit der pseudozufälligen Sequenz, die in Abhängigkeit des Geheimschlüssels der Gruppe generiert wurde, korreliert. Bei dem richtigen Fingerabdruck wird die Korrelation nah dem Wert 1 sein, wenn das markierte Bild nicht vorher manipuliert wurde (siehe **Abb. 3**(b).

In Fall einer über mehrere Gruppen verteilten Attacke kann die Differenz der Korrelationswerte eventuell nicht ausreichen, um die Gruppe der Piraten zu identifizieren

4 Testen des Algorithmus

Um die Koalitionssicherheit des Algorithmus zu überprüfen, wurden 13 Bilder im .bmp Format mit 20 ACC Fingerabdrücken [Wu05] für 6 verschiedene Gruppen markiert und getestet, insgesamt also 1560 Bilder. Es wurden folgende Szenarien betrachtet:

1. Detektion der Fingerabdrücke ohne Koalitionsattacke
2. Detektion der Fingerabdrücke mit einer intra-Gruppe Koalitionsattacke
3. Detektion der Fingerabdrücke mit einer inter-Gruppe Koalitionsattacke

Ziel war es, mindestens einen der bei der Attacke beteiligten Piraten zu identifizieren.

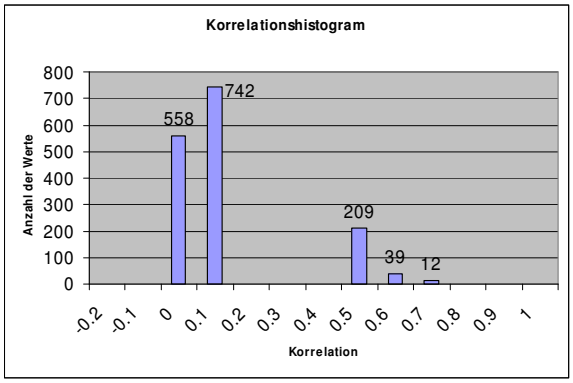
4.1 Detektion der Fingerabdrücke ohne Koalitionsattacke

Die **Abb. 3**(a) zeigt das Korrelationshistogramm der gesamten markierten Bilder, die, zuerst ohne Attacke, nach der richtigen Gruppierung getestet wurden. Das Bild zeigt das Ergebnis für einen der 6 Geheimschlüssel. Wie zu erwarten war, liegt der Korrelationswert für 260 Bilder über 0.45. Diese Werte gelten für die Bilder, die zur Gruppe des gewählten Geheimschlüssels gehören. Alle andere Bilder, die zu den restlichen 5 Gruppen gehören, zeigen niedrigere Korrelationswerte (<0.2). Im Fall der Verfolgung eines illegal verbreiteten Bildes wäre es damit deutlich zu erkennen, von welcher Gruppe das Bild stamm. Wie schon im vorherigen Kapitel erwähnt, ist die Detektion der Gruppe zuerst von den eingebetteten Fingerabdrücken unabhängig, sodass auch eine Koalitionsattacke innerhalb der Gruppe die Werte der detektierten Korrelation nicht beeinflussen würde.

Die **Abb. 3**(b) zeigt dagegen die Distribution der Korrelationswerte bei der Detektion der einzelnen Fingerabdrücke innerhalb einer Gruppe. Wie im **Abb. 3**(a), handelt es sich hier um Bilder, die nicht manipuliert wurden. Die 5200 Korrelationswerte entstanden bei der Überprüfung der 260 markierten Bilder, die jeweils mit den 20 Fingerabdrücken abgefragt wurden.

Wie zu erwarten ergaben nur 260 der Überprüfungen den Wert 1. Hier fand die Überprüfung mit dem richtigen Fingerabdruck statt. Der Unterschied zu den unkorrelierten Ergebnissen (< 0.4) ist hier hoch, so dass auch im Fall einer Koalitionsattacke gute Detektionsmöglichkeiten zu erwarten sind.

a)



b)

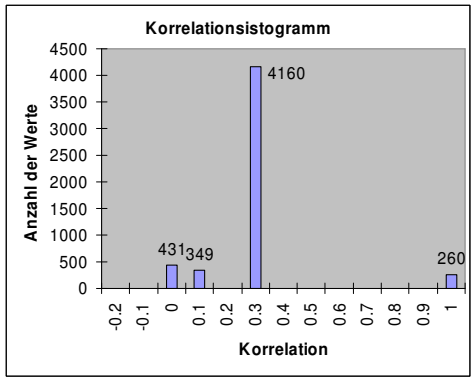


Abb. 3: Korrelationshistogramme für die Gruppenabfrage (a) und die Fingerabdruckabfrage (b)

4.2 Detektion nach einer intra-Gruppe Koalitionsattacke

Drei wahrscheinliche Angriffe auf markierten Bildern wurden simuliert: die Durchschnitts-, die Maximalwert- und Minimalwert-Attacke. Die Tests wurden zuerst mit zwei Bildern aus einer Gruppe simuliert. Es wurden 8 attackierte Bilder generiert jeweils mit den drei Attacken. Die bei dem Teilprozess B4) berechneten Korrelationswerte zeigen bei allen Bildern und Art der Attacke eine typische Verteilung, die im **Abb. 4** zu sehen ist. Die in der Abbildung mit * markierten Fingerabdrücke f1* und f2* sind die tatsächlich bei der Attacke beteiligten Fingerabdrücke, deren Korrelationswerte deutlich über den Rest liegen. In Fall einer intra-Attacke mit zwei Piraten wäre es so möglich, beide Piraten zu identifizieren.

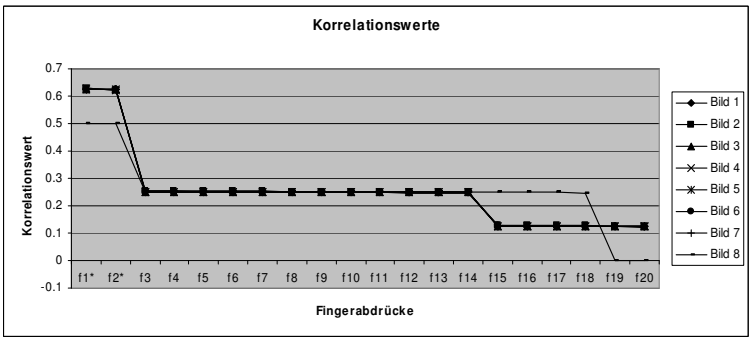


Abb. 4: Fingerabdruckabfrage in einer intra-Attacke von zwei Piraten

Die **Abb. 5** zeigt die Korrelationswerte in Fall einer intra-Attacke mit 3 und 4 Piraten. Die Legende der Abbildung zeigt in welcher Reihenfolge die Bilder kombiniert wurden, um das resultierende attackierte Bild zu produzieren. „(f1f20)f10“ bedeutet z.B. dass das mit Fingerabdruck f1 markierte Bild mit dem mit „f20“ markierten Bild zuerst in einer Durchschnittattacke kombiniert wurden. Das Ergebnis davon wurde dann noch mit dem mit f10 markierten Bild kombiniert. Die berechneten Korrelationswerte widerspiegeln die Gewichte der Bilder

bei der Durchschnittattacke. Das Diagramm zeigt, dass auch in diesem Fall mindesten die Korrelationswerte eines bei der Attacke beteiligten Fingerabdruckes deutlich höher als die andere liegt. Das würde die Identifikation des Piraten ermöglichen.

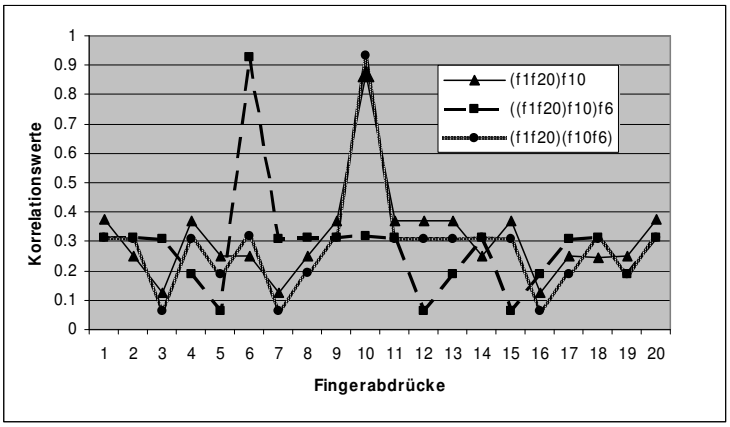


Abb. 5: Fingerabdruckabfrage in einer intra-Attacke von mehreren Piraten

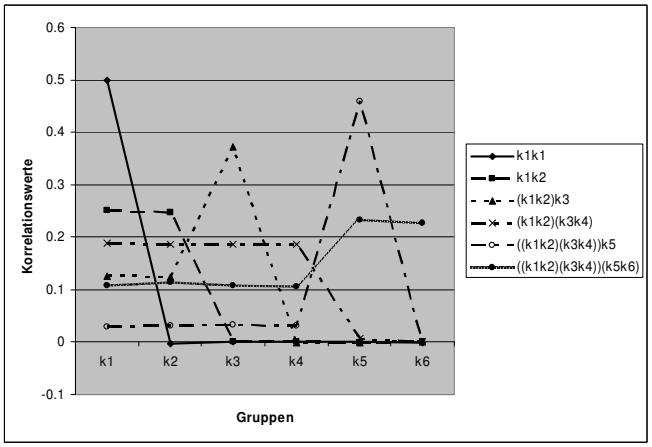


Abb. 6: Gruppenabfrage in einer inter-Gruppe Attacke aus mehreren Gruppen

4.3 Detektion nach einer inter-Gruppe Koalitionsattacke

Die **Abb. 6** zeigt die Relation zwischen der Anzahl der an einer Attacke beteiligten Gruppen und die Korrelationswerte bei der Gruppenabfrage. Die Legende des Bildes zeigt in welcher Reihenfolge die Bilder kombiniert wurden, um das resultierende attackierte Bild zu produzieren. „(k1k2)k3“ bedeutet z.B. das ein markiertes Bild aus der ersten Gruppe mit einem markierten Bild aus der zweiten Gruppe zuerst in einer Durchschnittattacke kombiniert wurden. Das Ergebnis davon wurde dann noch mit einem markierten Bild aus der dritten Gruppe kombiniert. Die berechneten Korrelationswerte widerspiegeln die Gewichte der Bilder bei der Durchschnittattacke. Sind Piraten aus nur zwei oder drei Gruppen bei der Koalitionsattacke beteiligt, kann man das bei der Detektion der Gruppe noch deutlich erkennen. Aus dem Diagramm kann man aber auch sehen, dass je mehr Gruppen beteiligt sind, desto unsicherer können die Korrelationswerte interpretiert werden.

In der Praxis bedeutet das, dass man die Überprüfung der Fingerabdrücke doch für alle Gruppen durchführen muss.
Die **Abb. 7** stellt die Ergebnisse der Korrelationswerte bei der Fingerabdruckabfrage im Fall einer inter-Gruppe Attacke aus mehreren Gruppen dar. Zur Abbildungslegende: „f01k1_f09k2 k1“ bedeutet, dass der Pirat mit Fingerabdruck f01 der Gruppe mit Geheimschlüssel k1 und der Pirat mit Fingerabdruck f09 der Gruppe mit Geheimschlüssel k2 bei der Attacke beteiligt waren. Durch eine zuvor geführte Gruppenabfrage konnte man feststellen, welche Gruppen beteiligt waren, sodass man die Fingerabdruckabfrage mit Geheimschlüssel k1 und k2 berechnet konnte. Aus dem Diagramm ist es zu lesen, dass man für die beiden getesteten Bilder („f01k1_f09k2“ und („(f01k1_f09k2)f18k3“) im Fall einer ähnlichen Attacke alle beteiligten Piraten identifizieren könnte.

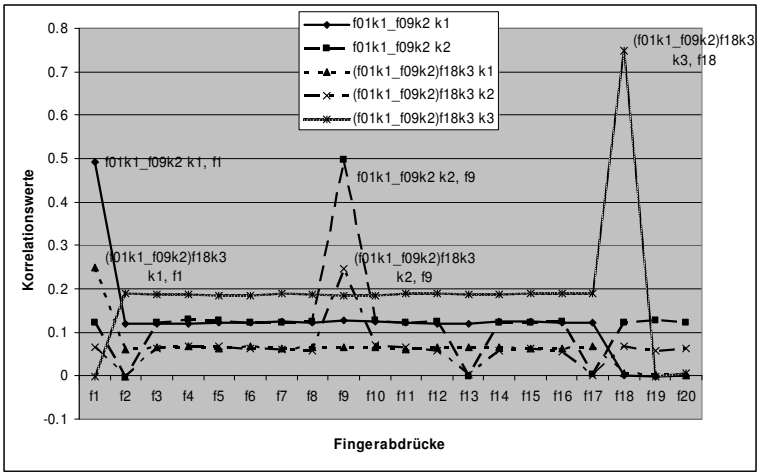


Abb. 7: Fingerabdruckabfrage in einer inter-Gruppe Attacke aus mehreren Gruppen

5 Zusammenfassung und Ausblick

Bei der vorliegenden Arbeit wurde ein koalitionssicherer Fingerabdruckalgorithmus vorgestellt, der die Idee der Gruppenbildung verwendet. Das eingebettete Wasserzeichen beinhaltet die Informationen bezüglich der Fingerabdrücke, die mit Hilfe von Anti-Koalitionscodes erzeugt werden, und bezüglich der Gruppenangehörigkeit, die mit einem Geheimschlüssel pro Gruppe festgelegt wird. Der Abfrageprozess detektiert zuerst die Gruppenangehörigkeit und dann die eingebetteten Fingerabdrücke mittels einer Korrelationsberechnung. Der größte Vorteil dieses Algorithmus ist, dass die Kapazität des Wasserzeichenprozess nicht mit der Anzahl der Kunden steigen muss. Neue Kunden bedeuten zuerst neue Gruppen mit neuen Geheimschlüsseln aber die Wasserzeichenlänge ist davon unhabhängig.
In diesem Arbeit geht man davon aus, dass eine intra-Gruppe Koalitionsattacke wahrscheinlicher ist als eine inter-Gruppe Attacke. In diesem Fall ist die Komplexität des Abfragealgorithmus am niedrigsten. Man konnte in allen getesteten Fällen das Ziel erreichen, dass mindesten ein der Piraten identifiziert wurde, auch wenn mehrere an der simulierten Attacke beteiligt waren. Ist doch eine inter-Gruppe Attacke aufgetreten, kann man trotzdem mit einem größeren Aufwand immer noch die beteiligten Piraten identifizieren.

Zusätzliche Testphasen sind geplant, um die Sicherheit des Algorithmus und seine Grenzen tiefer zu überprüfen und festzulegen. Diese Tests werden auf eine größere Anzahl von Bildern durchgeführt und werden auf eine Kombination von verschiedenen Koalitionsattacken mit zusätzlichen Bildbearbeitungsoperationen, wie Änderungen der Helligkeit oder des Kompressionsfaktors basieren.

Danksagung

Die Arbeiten und Ergebnisse, die in dieser Veröffentlichung beschrieben sind, werden teilweise von der Europäischen Kommission innerhalb des IST Programms, Vertrag IST-2002-507932 *ECRYPT*, unterstützt.

Literatur

[BoSh98] Dan Boneh, James Shaw: „Collusion-Secure Fingerprinting for digital data"; IEEE Transactions on Information Theory 44 (5): 1897-1905 (1998)

[CBK02] P. Cano, E. Batlle, T. Kalker, and J. Haitsma. A review of algorithms for audio fingerprinting; In International Workshop on Multimedia Signal Processing, US Virgin Is-lands, December 2002

[DFHJ00] Josep Domingo-Ferrer, Jordi Herrera-Joancomarti. "Simple Collusion-Secure Fingerprinting Schemes for Images," *itcc*, The International Conference on Information Technology: Coding and Computing (ITCC'00), 2000, p. 128

[HeWu05] Shan He, Min Wu: Group-Based Joint Coding and Embedding Technique for Multimedia Fingerprinting; Proceedings of the SPIE, Volume 5681, pp. 96-105 (2005).

[StCr05] Martin Steinebach, Lucilla Croce Ferri: „Einsatzgebiete nicht-blinder Wasserzeichen"; D-A-CH-Security 2005; Darmstadt; 15.-16. 3.2005

[TWWL03] W. Trappe, M. Wu, Z. Wang, K.J.R. Liu, "Anti-Collusion Fingerprinting for Multimedia," IEEE Trans. on Sig. Proc., Special issue on Data Hiding in Digital Media & Secure Content Delivery, 51 (4), pp.1069-1087, April 2003

[WTWL04] M. Wu, W. Trappe, Z. Wang, and K.J.R. Liu: "Collusion Resistant Fingerprinting for Multimedia", IEEE Signal Processing Magazine, Special Issue on Digital Rights Management, pp.15-27, March 2004

[Wu05] Yongdong Wu: Linear Combination Collusion Attack and its Application on an Anti-Collusion Fingerprinting; 2005 IEEE International Conference on Acoustics, Speech, and Signal Processing, March 18-23, 2005, Philadelphia, PA, USA

[WWTL04] Z. Wang, M. Wu, W. Trappe, and K.J.R. Liu: "Group-Oriented Fingerprinting for Multimedia Forensics", EURASIP Journal on Applied Signal Processing, Special Issue on Multimedia Security and Rights Management, Nov. 2004