Bildforensische Verfahren zur Unterstützung von Wasserzeichendetektion

Martin Steinebach, Christoph Moebius, Huajian Liu

TAD / Merit
Fraunhofer SIT
Rheinstrasse 75
64295 Darmstadt
martin.steinebach@sit.fraunhofer.de
huajian.liu@ sit.fraunhofer.de

Abstract: Digitale Bildwasserzeichen können oft durch Angriffe wie Skalierung und Rotation gestört werden. Zwar wird dabei das Wasserzeichen nicht entfernt, aber ein Auslesen wird deutlich erschwert, da keine Synchronisierung zwischen Trägersignal und Ausleseverfahren mehr möglich ist. Wir stellen hier einen Lösungsweg vor, der Elemente der Bildforensik zur Unterstützung des Ausleseprozesses heranzieht. Eine Skalierungsfaktor wird durch ein forensisches Verfahren abgeschätzt und an das Wasserzeichenverfahren übergeben, welches dann Schritt zum Rückgängigmachen der Skalierung durchführen und so erfolgreich das Wasserzeichen auslesen kann.

1 Motivation

Digitale Wasserzeichen werden heute in einer Reihe von Anwendungen eingesetzt, in erster Linie zum Schutz von Urheberrechten. Sie sind dem reinen Forschungsstadium entwachsen und hinsichtlich ihrer Eigenschaften wie insbesondere Robustheit und Transparenz soweit entwickelt, dass die Anforderungen eines Einsatzes in der Praxis erfüllt werden können. Allerdings gibt es auch noch immer Bedenken über eine effiziente Nutzbarkeit entsprechender Verfahren, da es teilweise leicht erscheint, das Auslesen von Wasserzeichen zu verhindern [Co02]. Ein verbreitetes Beispiel hierzu ist die Skalierung von Bildern: Viele Wasserzeichenverfahren basieren darauf, statistische Eigenschaften von Bildabschnitten miteinander zu vergleichen. Eine Skalierung des Bildes kann das Verfahren empfindlich stören, da der Algorithmus beim Auslesen nicht mehr die ursprünglichen Bildabschnitte erkennen kann, da deren Größe sich in einem für ihn unnachvollziehbarem Maß verändert hat. Einzige Möglichkeit, hier trotzdem erfolgreich ein Wasserzeichen auszulesen, ist bisher entweder ein Verfahren zu entwickeln, welches durch die Skalierung nicht gestört wird oder aber zu versuchen, die Skalierung durch Austesten potentieller Skalierungsschritte rückgängig zu machen. Der erste Weg erfordert neue Verfahren und ist dementsprechend aufwändig, der zweite Weg

führt zu einem langwierigen Ausleseprozess und kann die Verwendung des Wasserzeichenverfahrens in einigen Applikationen verhindern.

Wir stellen daher einen dritten, alternativen Weg vor, der als eine Verbesserung des Austestens der Skalierungsfaktoren angesehen werden kann: Auf Basis forensischer Analysen wird ein wahrscheinlicher Skalierungsfaktor berechnet, und dieser wird dann verwendet, um die Skalierung rückgängig zu machen und das Wasserzeichen auszulesen. So wird eine Robustheit gegen Skalierungen erreicht, ohne spezielle neue Verfahren im Wasserzeichenbereich entwickeln zu müssen, welche gegebenenfalls wiederum Nachteile in anderen Bereichen gegenüber heute eingesetzten Verfahren aufweisen können. Die diesem Vorgehen zugrunde liegende Idee, Forensik und Wasserzeichen zu verknüpfen, wird von uns allgemein in [TL+07] diskutiert.

2 Grundlagen

Das vorgestellte Verfahren basiert auf der Kombination von digitaler Forensik und einem digitalen Wasserzeichenverfahren. Beide Technologien sollen im Folgenden kurz vorgestellt werden. Dabei wird besonderes Augenmerk auf die Thematik der Skalierung gelegt.

2.1 Digitale Wasserzeichen

Der Ursprung der digitalen Wasserzeichen ([CMB02], [Di00]) liegt in der Steganographie, in beiden Technologien versucht man, Informationen unsichtbar in ein Trägermedium zu integrieren. Während Steganographie die Vertraulichkeit der eingebetteten Daten garantieren soll, werden Wasserzeichen primär eingesetzt, um die Authentizität und/oder Integrität eines Mediums überprüfen zu können oder das Urheberrecht zu schützen. Dabei unterscheiden sich die gewählten Verfahren teilweise stark, großen Einfluss hierauf haben die angestrebten Schutzziele oder Anwendungen.

Wir verwenden im weiteren Verlauf ein von uns entwickeltes Verfahren. Zur Einbettung des Wasserzeichens wird die Information nicht in Bildpunkte eingebracht, sondern in die Wavelet Koeffizienten eines in Blöcke geteilten Bildes. Ein visuelles Modell und ein externer Parameter bestimmen hierbei die Stärke, mit der das Wasserzeichen eingebracht wird. Je größer die Einbettungsstärke, desto robuster ist das Wasserzeichen. Gleichzeitig erhöht sich dabei aber auch der Einfluss des Wasserzeichens auf die Bildqualität; die Transparenz des Verfahrens nimmt ab.

Vorteile des Verfahrens sind eine hohe Robustheit gegen verlustbehaftete Kompression, wie beispielsweise JPEG, eine hohe Robustheit gegen das Überschreiben von Teilbereichen und eine gute Robustheit gegen Farb-, Helligkeits-, und Kontrastanpassungen. Allerdings sind auch die folgenden Nachteile zu beobachten: Das Verfahren weist eine hohe Komplexität auf und ist sehr anfällig gegen geometrische Transformationen wie beispielsweise Skalierung, Rotation und Scherung.

2.2 Anfälligkeit digitaler Wasserzeichen gegen Skalierung

Die Anfälligkeit digitaler Wasserzeichen gegen geometrische Transformationen ist leicht nachvollziehbar: Zum Auslesen eines Wasserzeichens muss das Detektionsverfahren mit dem Wasserzeichenstrom synchronisiert werden, d. h. es muss die Positionen im vorliegenden Trägermaterial identifizieren, die das Wasserzeichen beinhalten. Erhält ein Detektionsverfahren ein Bild unbekannter Herkunft und soll die Präsenz eines robusten Wasserzeichens prüfen, muss der Algorithmus berücksichtigen, dass das Bildmaterial evtl. nicht in seiner Originalform vorliegt, sondern mehreren Manipulationen ausgesetzt war. Schlägt der erste Detektionsversuch fehl, müssen sämtliche Bildveränderungen in Betracht gezogen werden, die das Verfahren tolerieren soll.

Für die folgenden Überlegungen gehen wir davon aus, dass die Teile der Wasserzeicheninformation in einem Bild aus 800 × 600 Pixeln im Abstand von 20 Pixeln (horizontal/vertikal) eingebettet wurden und zum Auslesen des Wasserzeichens mindestens die Hälfte dieser Einbettungspositionen korrekt ausgelesen werden müssen. Im ersten Detektionsversuch wird davon ausgegangen, dass das Bild in der Originalform vorliegt. Ist kein gültiges Wasserzeichen festzustellen, müssen alle Skalierungsfaktoren durchprobiert werden, die potentiell die korrekte Ausleseposition bieten. Gehen wir davon aus, dass wir uns mit einer Robustheit gegen Skalierung von 50% bis 200% der Originalgröße begnügen, kann ein vorgefundenes Bild von 800 x 600 Pixeln ursprünglich zwischen 400 x 300 und 1600 x 1200 Pixeln groß gewesen sein. Das würde das Austesten von 1200 Skalierungsschritten zwischen 400 und 1600 Pixeln auf der X-Achse erfordern. Dauert die Überprüfung pro Version eine Sekunde, muss mit einer Gesamtdauer von 1200 Sekunden, also 20 Minuten gerechnet werden. Diese Zeit fällt auch dann an, wenn gar kein Wasserzeichen vorhanden sein sollte. Denn in diesem Fall wird das Wasserzeichen über alle möglichen Varianten hinweg ergebnislos gesucht. Zu beachten ist, das wir hier nur von einer linearen Skalierung ausgehen, wird das Bild verzerrt, also X- und Y-Achse unterschiedlich skaliert, wächst der Suchaufwand exponentiell an.

An diesem kurzen Beispiel kann man erkennen, welcher zeitliche Aufwand das Auslesen eines Wasserzeichens bedeutet, wenn dem Detektionsverfahren das Original nicht vorliegt. Die Bedeutung dieser Problematik wird auch durch die Vielzahl von Veröffentlichungen zum Thema belegt, einige Beispiele hierfür sind [PP00], [RP98], [LW+01], [Ku98], [AM03] und [KH+03].

2.3 Digitale Bildforensik

Digitale Bildforensik versucht, anhand eines Bildes festzustellen, ob und wie es manipuliert wurde. Diese Aufgabe ist naturgemäß äußerst komplex; um eine Fälschung zu erkennen, muss man in den meisten Fällen die Vorgehensweise des Fälschers kennen. Zudem kann man im Allgemeinen nur Abschätzungen durchführen. Ein verbreitetes Beispiel ist das Erkennen einer sogenannten cloning-Modifikation. Hierbei werden Teile des Originals mit Kopien anderer Bereiche des gleichen oder eines fremden Bildes überschrieben, um eine andere Bildaussage zu erzielen. Ist auf der Fotografie eine

Person zu sehen, die vor einem regelmäßigen Hintergrund steht, so können Teile des Hintergrundes repliziert worden sein, um eine zweite Person zu verdecken. Ein forensischer Ansatz würde hier versuchen, identische Stellen im Bild aufzuzeigen und so einen Hinweis darauf zu geben, dass eine potentielle Modifikation vorliegt.

2.4 Erkennung von Bildskalierungen

In der vorliegenden Arbeit wird ein Teilbereich, die Erkennung von Bildskalierungen betrachtet. Wird ein digital gespeichertes Bild in seiner Größe verändert, so muss die Anzahl der Pixel an die neue gewünschte Größe angepasst werden. Will man es verkleinern, so müssen etliche der Originalbildpunkte entfernt werden. Will man es vergrößern, so müssen die Originalbildpunkte räumlich auseinander gerückt und die entstandenen Lücken gefüllt werden.

Bei der Verkleinerung eines Bildes geht Information verloren, weswegen schwieriger ist, diesen Vorgang nachzuweisen. Anders sieht es bei Vergrößerungen aus; hier wird neue Information generiert, um die Bereiche zwischen den Originalpixeln auszufüllen. Damit diese Bereiche sich möglichst gut in das Bild einfügen, benutzt man Interpolationsverfahren, um aus den umliegenden Bildpunkten den Farbwert des fehlenden Pixels zu bestimmen.

Im weiteren Verlauf der Arbeit sprechen wir ausschließlich die Skalierung auf ein größeres als das ursprüngliche Format an, eine Verkleinerung kann mit der gewählten Erkennungsstrategie nicht nachvollzogen werden. Allerdings kann davon ausgegangen werden, dass die digitale Bildforensik auch Lösungen für das Erkennen von Verkleinerungen vorstellen wird, mit denen dann analoge Lösungswege vorgestellt werden können.

Wenn bekannt ist, dass für die Interpolation der Randpixel nur der linke und der rechte Nachbar genutzt wurden und das arithmetische Mittel Anwendung fand, so kann man die interpolierten Bildpunkte relativ einfach von Originalpixeln unterscheiden. Die Differenz des linken Nachbarn eines Pixels und die Differenz eines Pixels mit seinem rechten Nachbarn ist dann gleich, wenn es sich bei dem Farbwert des Pixels um den Durchschnitt der beiden Nachbarn handelt.

Dieses Vorgehen ist sehr anschaulich, aber es lässt sich nur bedingt in der Praxis einsetzen. Einerseits kennt man das Interpolationsverfahren üblicherweise nicht, andererseits funktioniert es nur bei der Einfügung von "`ganzen"' Pixeln. "`Ganze"' Pixel bedeutet, dass zwischen zwei Originalbildpunkten ein neues Pixel eingefügt wird und die Originalpunkte vollständig erhalten bleiben. Das ist aber nur in den seltensten Fällen möglich.

Angenommen, wir wollen ein eindimensionales Bild von Größe 3 auf Größe 5 skalieren. Dies ist sehr einfach umzusetzen, indem nach dem ersten und dem zweiten Originalpixel je ein interpolierter Bildpunkt eingefügt wird. Bei einer Vergrößerung auf Größe 4 geht das nicht mehr so einfach. Es ist zu entscheiden, ob man nach dem zweiten oder nach dem dritten Originalpixel ein neues einfügt. Beide Varianten führen zu Verzerrungen im

Bild, weshalb dieses Vorgehen in der Praxis nicht praktikabel ist. In einem solchen Fall empfiehlt es sich, nach jedem Originalpixel drei neue Pixel einzufügen, die Interpolation durchzuführen und anschließend jeden dritten Bildpunkt auszuwählen. Diese ausgewählten Punkte ergeben dann das vergrößerte Bild.

Bei diesem Vorgang gehen Information verloren. In den vergrößerten Bildern verschwinden dadurch Originalpixel, man würde dementsprechend keinen interpolierten Bildpunkten finden.

Um diese Probleme zu vermeiden, kann man den Expectation-Maximization- oder kurz EM-Algorithmus verwenden, wie es in [Po04] vorgeschlagen wird. Dieser statistische Algorithmus wurde in [DLR77] vorgestellt. Er versucht in unserem Anwendungsfall jedes Pixel einem von zwei Modellen zuzuordnen: Das Modell 1 enthält dabei, grob gesagt, alle Punkte, die aus den Bildpunkten in der Umgebung interpoliert wurden, während das Modell 2 alle Punkte enthält, die unabhängig von ihren Nachbarn erscheinen.

3. Re-Synchronisierung durch Forensik

Zielsetzung ist, eine Verbesserung der Detektionsgeschwindigkeit bei robusten Bildwasserzeichen durch Einsatz digitaler forensischer Verfahren zu erreichen. Hierzu wird eine Software entwickelt, die im Folgenden auch Analysewerkzeug genannt wird.

3.1 Herausforderung und Fragestellungen

Um sicherzustellen, dass die erarbeitete Lösung auf eine große Menge an Material angewendet werden kann, muss eine Basis geschaffen werden, die viele aktuelle Bildformate verarbeiten kann. Auf dieser Basis ist anschließend eine geeignete Methode der Bildforensik zu implementieren, die eine Untersuchung auf Bildskalierungen ermöglicht.

Für die Verbesserung der bestehenden Wasserzeichendetektionsverfahren ist es allerdings nicht ausreichend, zu wissen, ob ein Bild skaliert wurde oder nicht. Vielmehr muss eine Abschätzung des Skalierungsfaktors durchgeführt werden, die über eine ausreichende Genauigkeit verfügt, um ein Auslesen des Wasserzeichens nach einer Re-Skalierung zu ermöglichen. Dazu muss das Verfahren in den Ausleseprozess des bereits vorhandenen Wasserzeichen-Verfahrens integriert werden.

Weiterhin sind die folgenden Fragen von Bedeutung:

- Wie genau ist die Abschätzung des Skalierungsfaktors im Allgemeinen?
- Welche Einflüsse haben der Bildinhalt, das Bildformat, sowie der verwendete Skalierungsfaktor auf die Genauigkeit der Schätzung?

- Wie hoch ist der tatsächliche Performance-Gewinn bei der Wasserzeichendetektion?

- Beeinflussen die verwendeten Wasserzeichenverfahren die Genauigkeit der Abschätzung?

Ihre Beantwortung bestimmt maßgeblich, ob das konzipierte Verfahren in der Praxis Verwendung finden kann und als Alternative zu herkömmlichen Synchronisierungsmechanismen digitaler Wasserzeichen einsetzbar ist.

3.2 Approximation der Skalierung

Der Kern der Herausforderung liegt darin, ein Verfahren zu entwerfen, welches nicht nur bestimmen kann, ob eine Skalierung vorliegt, sondern auch, um welchen Faktor diese vorgenommen wurde. Um dies zu erreichen, wird dem bereits besprochenen EM-Algorithmus eine Funktion zur Abschätzung beigefügt.

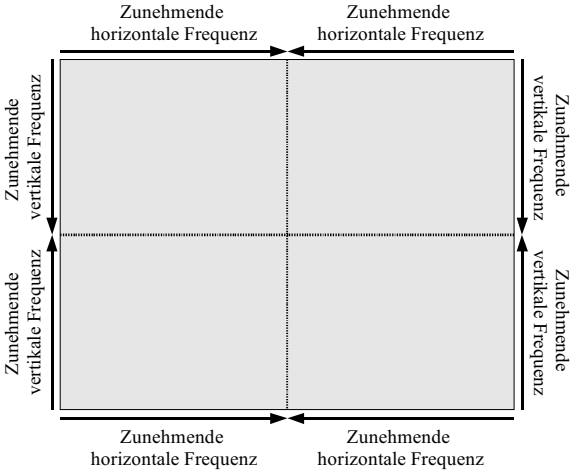

Abbildung 1: Veranschaulichung der FFT Funktion und ihrer Zuordnung

Die Approximation findet statt, nachdem die FFT-Darstellung der Probability Map angefertigt wurde. Diese Repräsentation besteht aus einem Graustufenbild, in welchem jeder Pixel einem Fourier-Koeffizienten entspricht. Je heller ein Bildpunkt, desto stärker ist die entsprechende Frequenz enthalten. Je weiter ein Punkt in der Mitte liegt, desto höher ist die Frequenz in der dazugehörigen Dimension; liegt ein Punkt horizontal in der Mitte, so ist die horizontale Frequenz hoch, liegt ein Punkt vertikal in der Mitte, so ist die vertikale Frequenz hoch. Aufgrund der Tatsache, dass die Frequenzen von außen zur Mitte hin immer höher und von der Mitte zum nächsten Rand wieder niedriger werden, kann sich die Heuristik auf die Hälfte jeder Achse der FFT-Darstellung, d. h. ein Viertel der erzeugten FFT-Repräsentation beschränken. Weiter sollten die besonders tiefen Frequenzen, die in jedem Bild in Form von großen einfarbigen Flächen auftreten können, ignoriert werden. Um das zu bewerkstelligen, werden an jeder Achse die ersten

zwei Prozent übersprungen. Daran anschließend muss die Heuristik zur Mitte hin nach der Frequenz suchen, deren Häufigkeit am meisten vom Durchschnitt abweicht.

Probability Maps von skalierten Bildern enthalten eine Art Gitter, das parallel zu den Bildrändern ausgerichtet ist, welches dadurch entsteht, dass sich interpolierte und nicht interpolierte Pixel sowohl horizontal wie auch vertikal abwechseln (siehe Abbildung 1). Deshalb ist nach möglichst reinen horizontalen und vertikalen Frequenzen zu suchen. Es bietet sich also an, von einer Ecke aus senkrecht nach oben oder unten und anschließend von derselben Ecke aus waagerecht nach rechts oder links nach Punkten zu suchen, deren Helligkeit sich von der Umgebung deutlich abheben. Kennt man die Position dieser herausragenden Fourier-Koeffizienten, kann man auf den Skalierungsfaktor in der jeweiligen Richtung schließen.

Durch Beobachtung bei einigen Testbildern wurde festgestellt, dass sich die am deutlichsten sichtbaren Markierungen, die in der FFT-Darstellung der Probability Maps von skalierten Bildern auftreten, im linken unteren Quadranten ansiedeln, weshalb die Approximationsheuristik von der linken unteren Ecke ausgehend nach den beiden Punkten suchen muss, die den Skalierungsfaktor widerspiegeln. Weiter zeigte die Untersuchung der Probability Maps von verschiedenen Bildern, dass die zu suchenden Markierungen in der jeweiligen Spalte oder Zeile der dunkelste Punkt der betrachteten Daten ist; in Extremfällen hat dieser die Farbe Schwarz (den Farbwert Null). Es wurde ein Vergleich zwischen der Suche nach dem dunkelsten Punkt und der Suche nach dem Punkt mit der größten Abweichung vom Mittelwert durchgeführt, welcher ergab, dass Erstere in vielen Fällen deutlich bessere Ergebnisse liefert als Letztere.

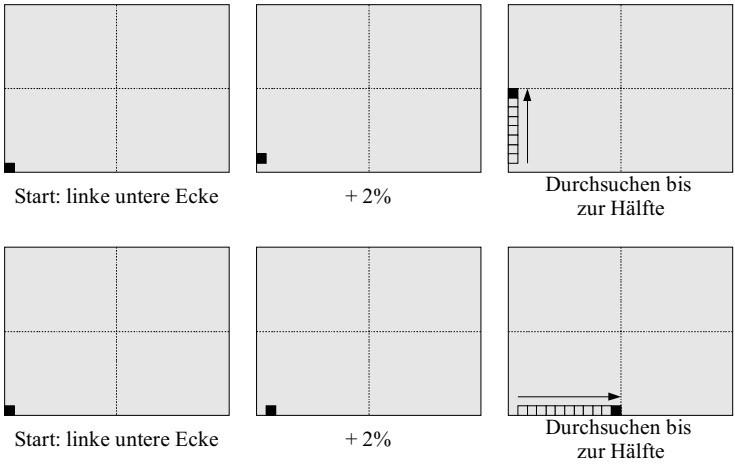

Abbildung 2: Ablauf der Abschätzung

Die Funktion, die den dunkelsten Punkt entlang des linken und entlang des unteren Randes der FFT-Darstellung sucht und den Abstand zur Ecke zurückgibt ist demzufolge das Herzstück der Approximation. Das erledigt eine Prozedur, deren Vorgehensweise in Abbildung 2 dargestellt ist. Existieren entlang der durchsuchten Strecke mehrere dunkelste Punkte, so wird derjenige gewählt, der am weitesten von der Ecke entfernt ist.

4. Implementierung

Um die Grundfunktionalität einer Bildverarbeitungsanwendung zu bieten, wird als Ausgangspunkt CxImage (http://www.xdp.it) verwendet. Hierbei handelt es sich um eine in C++ geschriebene Windows-Anwendung, die verschiedene Bildformate einlesen und speichern kann; zudem verfügt sie über kleinere Manipulationswerkzeuge. Für den forensischen Kern der bereits vorgestellte EM Algorithmus eingesetzt. Um die Implementierung möglichst portabel zu gestalten, arbeitet er intern mit einer Darstellung des Bildes als eindimensionales vorzeichenloses Integer-Array. Da CxImage Bildmaterial in Form eines Objekts vom proprietären Typ CxImage verwaltet, muss es zur Übergabe an das Analysemodul entsprechend umgeformt werden.
Zur Abschätzung des Skalierungsfaktors wird das Ergebnis des EM Algorithmus, die sogenannte Probability Map, analysiert. Hierbei sind die Frequenzen der geschätzten Wahrscheinlichkeiten zu bestimmen, die am häufigsten auftreten. Zur Unterstützung dieses Vorgangs wird die Probability Map per Fast-Fourier-Transformation (FFT) in den Frequenzraum überführt. Die Entscheidung, welche Frequenzen zur Abschätzung herangezogen werden, ist ein heuristischer Vorgang. Zur einfacheren Auswertung kann der Kontrast der Probability Map oder deren FFT-Darstellung angehoben werden.

In Abbildung 3 wird gezeigt, wie die einzelnen Komponenten miteinander verknüpft sind und welchen Weg zu analysierende Bildinformationen nehmen.

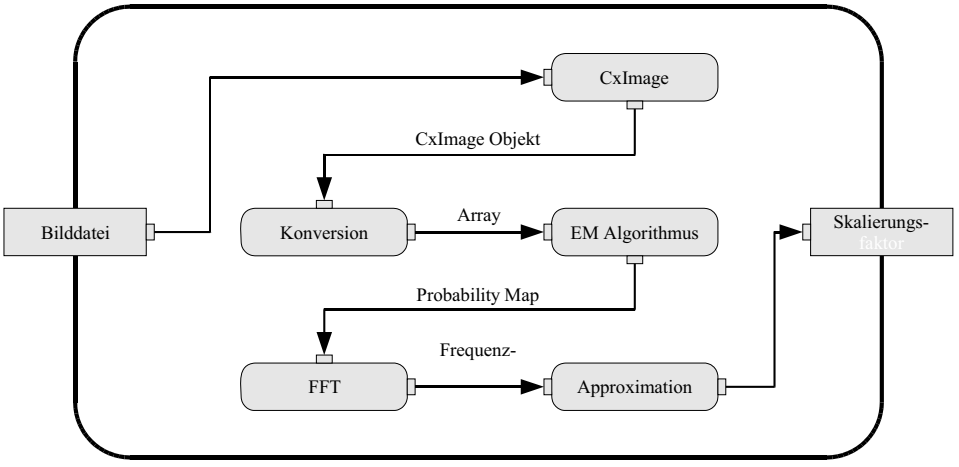

Abbildung 3: Aufbau des Lösungswegs

Da die Ausführung des EM Algorithmus sehr viel Speicherplatz und Verarbeitungszeit in Abhängigkeit von der Bildgröße verbraucht, wird der Multi Random Area Mode zur Verfügung gestellt. In diesem Modus selektiert das Analysewerkzeug per Pseudozufallsgenerator mehrere Bereiche aus dem Bild und führt für diese Bildausschnitte den EM Algorithmus mit den Standardwerten aus. Von den erzeugten Schätzungen des Skalierungsfaktors wird anschließend der Mittelwert gebildet. In Abbildung 4 ist eine grafische Darstellung des Vorganges zu sehen. Das hat den Vorteil, dass nicht das gesamte Bild und die erzeugten Berechnungsergebnisse, die während des EM Algorithmus anfallen, im Speicher gehalten werden müssen, sondern nur ein kleiner Bereich. Die Anzahl der Bereiche kann über die Benutzerschnittstelle festgelegt werden.

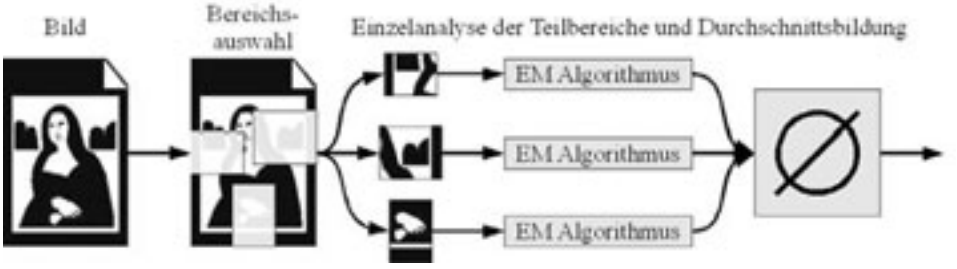

Abbildung 4: Multi Random Area Mode - Teile des Bildes werden analysiert und der Durchschnitt der Ergebnisse gebildet

5. Testergebnisse und Diskussion

In Tabelle 1 wird die Verbesserung der Ausleseerfolge für 50 markierte und anschließend skalierte Bilder gezeigt. Während ohne eine Abschätzung eine Skalierung nicht überstanden wird, können mit einer Abschätzung eine Vielzahl von Wasserzeichen wieder korrekt ausgelesen werden. Bei einem Skalierungsfaktor von 1,4 sind dies immerhin fast 70 Prozent der eingebetteten Wassereichen.

Tabelle 1: Detektionssteigerung durch Wasserzeichen

	ohne Abschätzung		mit Abschätzung	
Skalierung	Anzahl korrekte Detektionen	Korrekt %	Anzahl korrekte Detektionen	Korrekt %
1	50	100	50	100
1,1	0	0	0	0
1,2	0	0	16	32
1,3	0	0	6	12
1,4	0	0	34	68
1,5	0	0	23	46
1,6	0	0	14	28
1,7	0	0	22	44
1,8	0	0	0	0
1,9	0	0	0	0

Auffällig ist, dass gerade bei einer minimalen Skalierung von 1,1 keine Verbesserung erfolgt. Die niedrige Erfolgsrate wird ausschließlich in einer falschen Einschätzung durch die Forensik im Zusammenspiel mit dem Einbetten des Wasserzeichens begründet: Dieses ist nicht transparent für die Forensik, es werden Strukturen erzeugt, die fälschlicher Weise als Artefakte einer Skalierung gedeutet werden. Während das Wasserzeichen für alle Skalierungsfaktoren gleich stark ist, ist die Ausprägung der Skalierung proportional zu den Skalierungsartefakten. Demensprechend überlagern bei einer niedrigen Skalierung die Artefakte des Wasserzeichens die Artefakte der Skalierung und führen zu einer Fehlinterpretation der Skalierungserkennung. Dadurch wird die Re-Skalierung falsch durchgeführt und das Wasserzeichen kann nicht korrekt ausgelesen werden.

Abbildung 5 zeigt, dass die Skalierungserkennung gute Ergebnisse liefert und im Durchschnitt über 100 Bilder bei einer Skalierung zwischen Faktor 1,1 und 1,7 eine Fehlerrate von unter 10 Prozent liefert. Beachtenswert sind insbesondere die vergleichsweise hohen Fehlerraten, wenn keine Skalierung vorliegt. Folglich sollte eine Implementierung des Lösungsweges immer zuerst das Auslesen des Wasserzeichens ohne Skalierungskorrektur testen, da im Falle einer nicht durchgeführten Skalierung so der fehleranfällige Re-Skalierungsprozess umgangen wird, wenn das Wasserzeichen bereits im Vorfeld erfolgreich ausgelesen wird.

In Abbildung 6 werden die durchschnittlichen Erfolgsraten der Skalierungserkennung mit und ohne ein vorher eingebettetes Wasserzeichen miteinander vergleichen, hierbei werden 50 Bilder im Test verwendet. Dabei fällt auf, dass sich die durchschnittliche Genauigkeit in fast allen Fällen durch das eingebettete Wasserzeichen deutlich verschlechtert. Zu Begründen ist diese Verschlechterung dadurch, dass die Einbettung eine neue Periodizität in das Bildmaterial einbringt, da das Wasserzeichen blockweise und redundant in das Bild integriert wird.

Die Testergebnisse zeigen die prinzipielle Nutzbarkeit des Verfahrens, um eine gute Abschätzung der Skalierungsfaktoren durchzuführen. In vielen Fällen ist die Abweichung von den tatsächlichen Faktoren überraschend gering. Allerdings haben sich insbesondere Bilder, welche große einfarbige Flächen oder Bewegungsunschärfe durch bewegte Objekte bzw. Verwackeln der Kamera aufweisen, als Problemfälle herausgestellt. Dies ist kein unerwartetes Ergebnis, da derartige Fotografien Teile der Szenerie mehrfach enthalten (bewegte Objekte oder viele gleichfarbige Pixel), was sich in statistischen Zusammenhängen widerspiegelt. Diese Zusammenhänge können vom EM Algorithmus nicht von den Zusammenhängen, die in skalierten Bildern auftreten, unterschieden werden und hinterlassen Spuren in den entsprechenden Probability Maps. Die Spuren dann werden von der Approximationsheuristik fehlgedeutet.

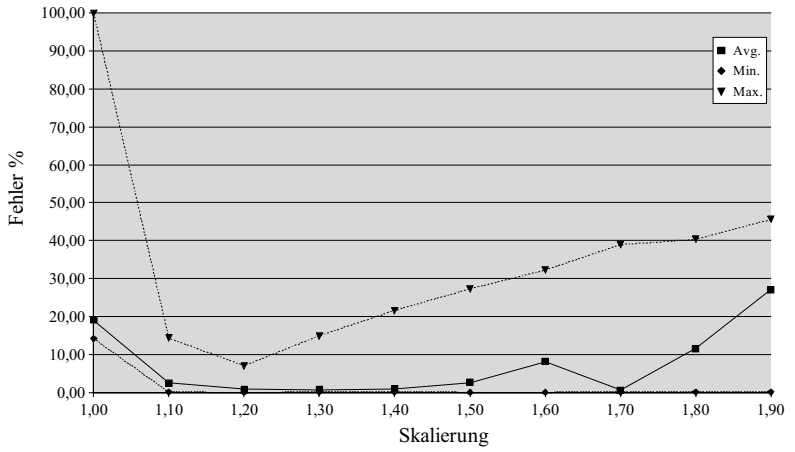

Abbildung 5: Skalierungsgenauigkeit für 100 Beispielbilder, jeweils skaliert mit den Faktoren 1,0 bis 1,9

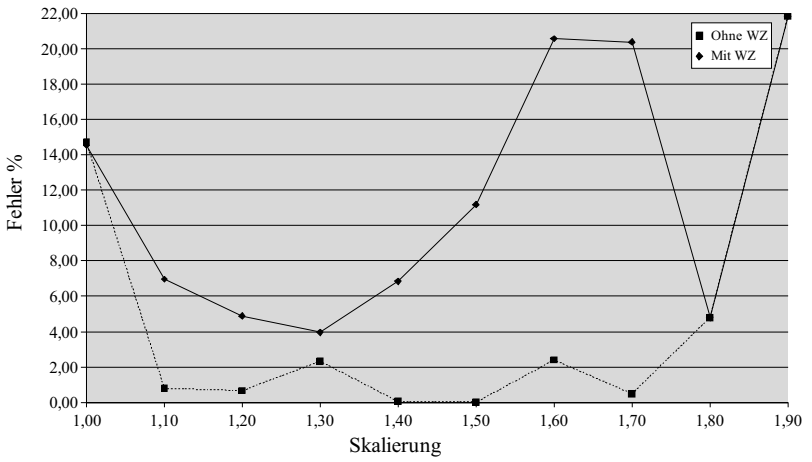

Abbildung 6: Auswirkungen des eingebetteten Wasserzeichens

Weitere Problemfälle sind Bilder, die unskaliert vorliegen. Hier weist das Verfahren die höchste maximale Abweichung von allen Schätzungen auf. Diese Abweichung entsteht nicht durch den EM Algorithmus, sondern durch die Art und Weise, wie die Approximationsheuristik die berechnete FFT-Darstellung der Probability Map auswertet.

Es wird deutlich, dass der Ansatz zu diesem Zeitpunkt noch Schwachstellen beinhaltet. Allerdings kann derzeit als einzige Alternative nur eine vollständige Suche nach Wasserzeichen über alle potentiellen Skalierungen hinweg durchgeführt werden, was zu einer nicht akzeptablen Komplexität der Detektion führen würde. Beschränkt man sich bei der systematischen Suche allerdings auf einen kleinen Bereich, so verliert das

Schätzverfahren durch seine lange Laufzeit an Attraktivität: Angenommen, man zöge für die Suche nur die Skalierungsfaktoren zwischen 1,0 und 1,9 in Betracht. Benutzt man ausschließlich das Detektionsverfahren, und prüft mit einer Schrittweite vom Faktor 0,1 in diesem Bereich die resultierenden Bilder auf Gültigkeit des Wasserzeichens, so würde man zehn Detektionsversuche benötigen. Unter der Voraussetzung, dass jeder Versuch etwa 10 bis 20 Sekunden dauert (diese Werte treffen für das verwendete WZ-Verfahren zu), könnte man den gesamten Bereich in maximal 200 Sekunden durchsuchen. Die Abschätzung des Skalierungsfaktors hingegen benötigt auf dem verwendeten Rechner pro Bild zwischen 5 und 10 Minuten, was im besten Fall immer noch langsamer als die systematische Suche ist.

6. Ausblick und Zusammenfassung

Wie wir gezeigt haben, bietet die Kombination von digitalen Wasserzeichen und digitaler Bildforensik vielversprechende Ansätze. Das vorgestellte Verfahren kann, wie in den Testreihen bestätigt, dazu beitragen, den Erfolg der Wasserzeichendetektion zu verbessern.

Trotz dieses positiven Fazits bleibt die Praxistauglichkeit vorerst jedoch eingeschränkt: Die vorgeschlagene Strategie kann nur zur Erkennung von Vergrößerungen von Bildern herangezogen werden. Die Genauigkeit der Schätzung leidet unter der Einbettung des verwendeten Wasserzeichens. Mit der erhöhten Abweichung von tatsächlichem und geschätztem Skalierungsfaktor kann in einigen Bildern die Wasserzeicheninformation nicht zuverlässig ausgelesen werden. Um die Abweichung auszugleichen, müssten nach einem missglückten Detektionsversuch systematisch alle benachbarten Skalierungsfaktoren in Betracht gezogen werden, was den Vorteil der vorherigen Abschätzung zunichte machen würde: Ist kein Wasserzeichen vorhanden, müsste man die Suche endlos fortsetzen oder sich auf einen Bereich von Skalierungsfaktoren beschränken.

Eine potentielle Verbesserung der Herangehensweise ist durch die Verwendung eines schnelleren Abschätzungsverfahrens denkbar. In [Ga05], [PR06] und [MS07] sind verschiedene Verfahren vorgeschlagen worden, die einen Geschwindigkeitszuwachs versprechen und in zukünftigen Untersuchungen auf die Verwendbarkeit in unserem vorgeschlagenen Verfahren untersucht werden müssen.

Als Ausblick muss auch noch in Betracht gezogen werden, dass auch die eingesetzten forensischen Verfahren genauer betrachtet werden müssen, wenn sie im Zusammenhang mit digitalen Wasserzeichen und Urheberschutz eingesetzt werden. So zeigen [GK+07] Möglichkeiten auf, entsprechende Verfahren zu umgehen. Im Falle eines bewussten Angriffs auf ein Wasserzeichen ist somit eine Maskierung des Angriffs selbst denkbar.

Literaturverzeichnis

[AM03] A. M. Alattar, J. Meyer, Watermark Re-synchronization Using Log-polar Mapping of Image Autocorrelation, Proceedings of the 2003 International Symposium on Circuits and Systems, ISCAS '03. vol. 2, pp. 928-931, 2003

[CMB02]Cox, Miller, Bloom; Digital Watermarking, Academic Press, San Diego, USA, ISBN 1-55860-714-5, 2002

[Co02] Cormac Herley. Why Watermarking is Nonsense, IEEE Signal Processing Magazine Sept. 2002.

[Di00] Dittmann; Digitale Wasserzeichen, Springer Verlag, ISBN 3 - 540 - 66661 - 3, 2000

[DLR77] A.P. Dempster, N.M. Laird, D.B. Rubin, Maximum-Likelihood from incomplete data via the EM algorithm. In Journal of the Royal Statistical Society, 1977.

[Ga05] Gallagher, Detection of linear and cubic interpolation in JPEG compressed images. In Proceedings of the Second Canadian Conference on Computer and Robot Vision, pp. 65-72, 2005

[GK+07] Gloe, T., Kirchner, M., Winkler, A., and Böhme, R. 2007. Can we trust digital image forensics?. In Proceedings of the 15th international Conference on Multimedia (Augsburg, Germany, September 25 - 29, 2007). MULTIMEDIA '07. ACM, New York, NY, 78-86

[KH+03] X. Kang, J. Huang, Y. Shi, Y. Lin, A DWT-DFT Composite atermarking Scheme Robust to Both Affine Transform and JPEG Compression“, IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 776-786, August 2003

[Ku98] M. Kutter, Watermarking Resistance to Translation, Rotation, and Scaling, Proc. SPIE Multimedia Systems Applications, vol. 3528, pp.423-431, 1998

[LW+01] C.-Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y.-M. Lui, “Rotation, scale, and translation resilientwatermarking for images,” IEEE Trans. Image Processing, vol. 10, pp. 767–782, May 2001.

[MS07] Mahdian, Saic, On periodic properties of interpolation and their application to image authentication. In Third International Symposium on Information Assurance and Security, pages 439-446, 2007

[Po04] Alin C. Popescu, Statistical Tools for Digital Image Forensics, Ph. D. Thesis, Dartmouth College, 2004.

[PP00] S. Pereia and T. Pun, “Robust template matching for affine resistant image watermarks,” IEEE Trans. Image Processing, vol. 9, pp. 1123–1129, 2000.

[PR06] Prasad, Ramakrishnan, On resampling detection and its application to detect image tampering. In Proceedings of the 2006 IEEE International Conference on Multimedia and EXPO (ICME 2006), pp. 1325-1328, 2006

[RP98] J. J. K. O’Ruanaidh and T. Pun, “Rotation, scale and translation invariant spread spectrum digital image watermarking,” Signal Processing, vol. 66, no. 3, pp. 303–317, 1998.

[TL+07] Thiemert, Liu, Steinebach, Croce-Ferri, Joint forensics and watermarking approach for video authentication, Security, Steganography, and Watermarking of Multimedia Contents IX, Edward J. Delp III, Ping W. Wong, Editors, ISBN: 9780819466181, SPIE / IS&T, Bellingham, 2007