Security and Safety Engineering

HOCHSCHULE FURTWANGEN UNIVERSITY HFU

Technische Schutzmaßnahmen gegen Produktpiraterie

SSB6 WS 2015/16

Erstellt von:

Müller, Hendrik 242777 Am Großhausberg 4 78120 Furtwangen

Abgabetermin:

Furtwangen, 19.02.2016

Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich die Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie Zitate kenntlich gemacht habe. Ich bin damit einverstanden, dass die Arbeit durch Dritte eingesehen und unter Wahrung urheberrechtlicher Grundsätze zitiert werden darf.

_____ _____

Ort, Datum

Hendrik Müller
Student

Kurzfassung

Produktpiraterie ist heute so aktuell wie nie. Immer wieder werden Unternehmen Opfer, indem ihre Produkte kopiert werden.
Um sich gegen Produktpiraterie zu schützen gibt es verschiedene Vorgehensweisen; von der Wahl der Materialien über den Prozessablauf bis hin zu rechtlichen Schritten. In dieser Arbeit sollen verschiedene technische Schutzmaßnahmen gegen Produktpiraterie vorgestellt werden. Vor allem im Maschinenbau kommt eine Vielzahl verschiedener Schutzmaßnahmen zum Einsatz, wovon viele auch in anderen Bereichen eingesetzt werden.
Im Folgenden sollen verschiedene Maßnahmen vorgestellt, auf ihre individuellen Eigenschaften hin untersucht und miteinander verglichen werden bzw. in Kategorien eingeteilt werden. Ziel ist eine nicht abschließende aber umfangreiche Liste mit verschiedenen technischen Maßnahmen gegen Produktpiraterie.

Abstract

Counterfeit is nowadays as relevant as ever. Companies are repeatedly falling victim to counterfeit because their products are being imitated.
There are several strategies to protect against counterfeit; from the choice of material and the process flow to legal actions. This paper shall present various different technical measures against counterfeit. Especially in mechanical engineering there are many different technical measures in use that are also common in other fields of production.
The following shall present various different technical measures, examine their individual characteristics and compare them with each other, respectively categorize them. The desired end state is a non-concluding but extensive and comprehensive list of a variety of different technical measures against counterfeit.

INHALTSVERZEICHNIS

Abkürzungsverzeichnis

CDP	Copy Detection Pattern
VDMA	Verband Deutscher Maschinen- und Anlagenbau e.V.

Abbildungsverzeichnis

Tabellenverzeichnis

Glossar

Weiche Plagiate	Kopien von Bedienungsanleitungen, Produktfotos, Kataloge etc. Nicht jedoch von den eigentlichen Produkten selbst (Verband Deutscher Maschinen- und Anlagenbau [VDMA], 2014).
Kennzeichnung	„Merkmal eines Produktes, […] um eine Unterscheidung von anderen Produkten vorzunehmen. Sowohl Merkmale des Produktes selbst, als auch zusätzlich angebrachte Merkmale können als Kennzeichnung dienen“ (Innovation mit Normen und Standards [INS], 2010; S. 3).
Verifizierung	„Zur Unterscheidung verschiedener Produkte im Rahmen einer Verifizierung gibt es Möglichkeiten der Identifizierung und der Authentifizierung“ (INS, 2010; S. 3).
Identifizierung	„[E]indeutige Unterscheidung eines bestimmten Produktes von allen anderen […] Produkten“ (INS, 2010; S. 3).
Authentifizierung	„[D]ie Unterscheidung/ Abgrenzung eigener Produkte („authentisch“) von den Produkten anderer („nicht authentisch“)“ (INS, 2010; S. 4).
Originalitätskennzeichen	„Kennzeichen […], welche fälschungssichere Merkmale enthalten und somit die Echtheit eines Produktes eindeutig nachweisen“ (Abele, Kuske & Lang, 2011; S. 42).
Unikatskennzeichen	Die Merkmale sind zusätzlich einmalig, was eine individuelle Zuordnung der Produkte erlaubt (Abele, et al. 2011).
Identitätskennzeichen	Können Informationen enthalten, aber kein Originalitäts-kennzeichen (Abele, et al. 2011).
Robustheit	„Hier wird eingeordnet, wie hoch die Robustheit des Trägers gegen Einwirkung von Feuchte, Hitze, Kälte, Vibrationen, Staub, Metallspäne, Schierstoffe, Betriebsstoffe, etc. innerhalb eines gegebenen Zeitraums ist“ (INS, 2010; S. 29).

1 Einleitung

Um sich gegen Produktpiraterie zu schützen gibt es eine Vielzahl an Möglichkeiten; von organisatorischen und technischen bis hin zu rechtlichen Maßnahmen. Dabei führt oft erst eine effektive Kombination all dieser Maßnahmen zu einer effektiven und übergreifenden Abwehr von Produktpiraterie (Staake & Fleisch, 2008).

In dieser Arbeit sollen die technischen Schutzmaßnahmen einmal genauer betrachtet werden. Vor allem im Maschinen- und Anlagenbau kommen vermehrt technische Schutzmaßnahmen (z.B. in Form von Produktkennzeichnungen) zum Einsatz (Günthner, Durchholz, Stockenberger, Wildemann, Pommer, Tschöke, et al., 2010). Diese können aber natürlich auch in anderen Bereichen zum Einsatz kommen.
Die am weitesten verbreiteten Maßnahmen sollen im Folgenden aufgeführt und vorgestellt werden. Dabei werden auch ein paar weniger verbreitete Maßnahmen vorgestellt. Die Maßnahmen sollen alle auf ihre individuellen Merkmale hin untersucht und kategorisiert werden. In einer umfassenden Tabelle sollen die verschiedenen Merkmale dann gegenübergestellt werden.

2 Zielsetzung

Ziel dieser Arbeit soll eine ausführliche, aber nicht abschließende Liste technischer Schutzmaßnahmen gegen Produktpiraterie sein. Diese Liste soll möglichst detailliert die verschiedenen Merkmale der verschiedenen Technologien beschreiben. Zusätzlich sollen Anforderungen an technische Schutzmaßnahmen vorgestellt und erläutert werden, wie man die passende Technologie für ein bestimmtes Produkt finden kann. Anschließend sollen die Ergebnisse für die Einbindung in Vorlesungsmaterialien aufbereitet und in geeigneter Weise dargestellt werden (Foliensatz zu den verschiedenen Maßnahmen).

Für die Erarbeitung wurden hauptsächlich einschlägige Studien herangezogen die sich mit dem Thema technische Schutzmaßnahmen befasst haben. Vor allem im Bereich des Maschinenbaus gibt es hierzu Quellen und Materialien. Auch Informationen von Herstellern und Anbietern von technischen Schutzmaßnahmen wurden, sofern verfügbar, mit eingebunden.

3 Überblick über die Entwicklung der Produktpiraterie in der Industrie

Zu Beginn soll zunächst ein kleiner Überblick über die Entwicklung der Produktpiraterie in der Industrie wiedergegeben werden.

Wie schon in den Jahren zuvor wurde vom Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA) auch 2014 wieder eine Studie zur Produktpiraterie veröffentlicht. Die Studie gibt unter anderem Aufschluss darüber, wie sich die Produktpiraterie in den vergangenen Jahren entwickelt hat, wie viele Unternehmen betroffen sind, welcher Schaden entstand und welche Maßnahmen von den Unternehmen getroffen werden. Der Fokus liegt hierbei jedoch auf dem Maschinen- und Anlagenbau, weshalb die statistischen Werte im Folgenden mit Bedacht zu betrachten sind.

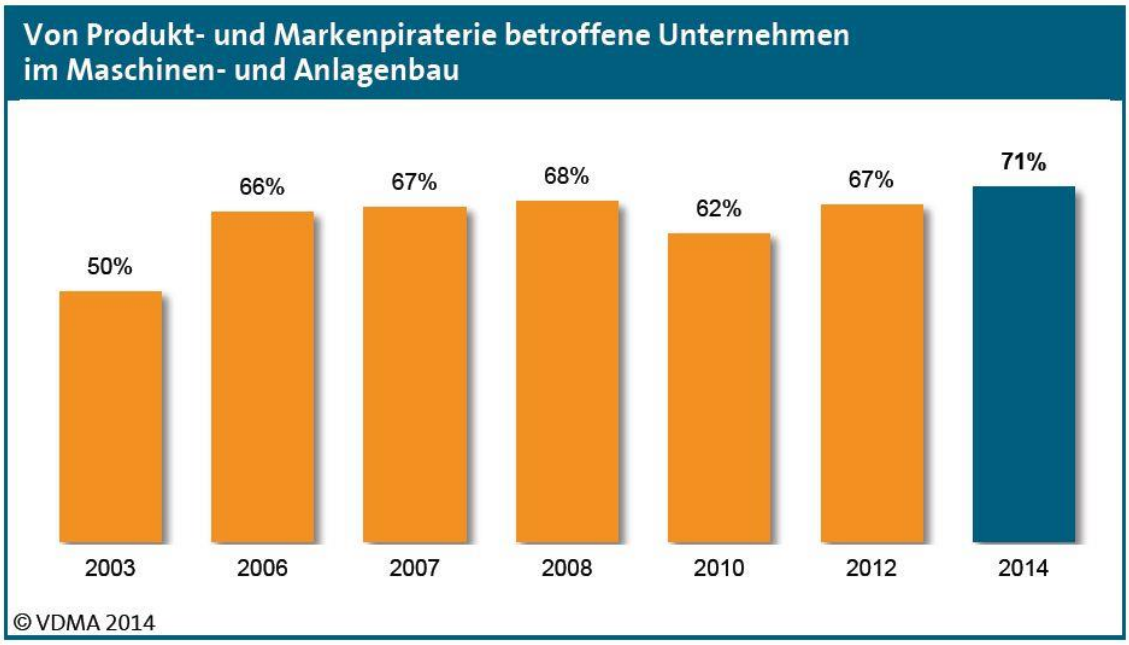

Abbildung 1: Von Produkt- und Markenpiraterie betroffene Unternehmen im Maschinen- und Anlagenbau (VDMA, 2014; S. 8).

An der neuesten Studie aus dem Jahre 2014 hatten sich insgesamt 337 Unternehmen beteiligt. Hierbei gaben 71% der Unternehmen an von Produkt- und Markenpiraterie betroffen zu sein (*siehe Abbildung 1*) und es wurde eine Schadenssumme von 7,9 Milliarden Euro vermerkt, die durch Produktpiraterie entstand (VDMA, 2014). Das entspricht ca. 38.000 Arbeitsplätzen. Im Vergleich zur vorangegangenen Studie aus dem Jahre 2012 ist somit ein Anstieg um ca. 1000 Arbeitsplätze zu erkennen, wobei die Schadenssumme konstant hoch

bleibt (Verband Deutscher Maschinen- und Anlagenbau [VDMA], 2012). Eine besondere Entwicklung ist dabei bei Plagiaten aus Deutschland zu erkennen. Insgesamt 23% der Plagiate stammen aus Deutschland, womit Deutschland direkt an zweiter Stelle hinter China mit 72% liegt. Allerdings handelt es sich bei den Plagiaten aus Deutschland meist um sogenannte „Hightech-Plagiate“. Insgesamt hat jedes vierte Unternehmen Probleme mit Reklamationen die von Plagiaten ausgehen (VDMA, 2014).

Am häufigsten kommen Schutzrechte als Präventivmaßnahme zum Einsatz. Lediglich 38% der Unternehmen setzen auch auf technische Schutzmaßnahmen wie in *Abbildung 2* zu sehen.

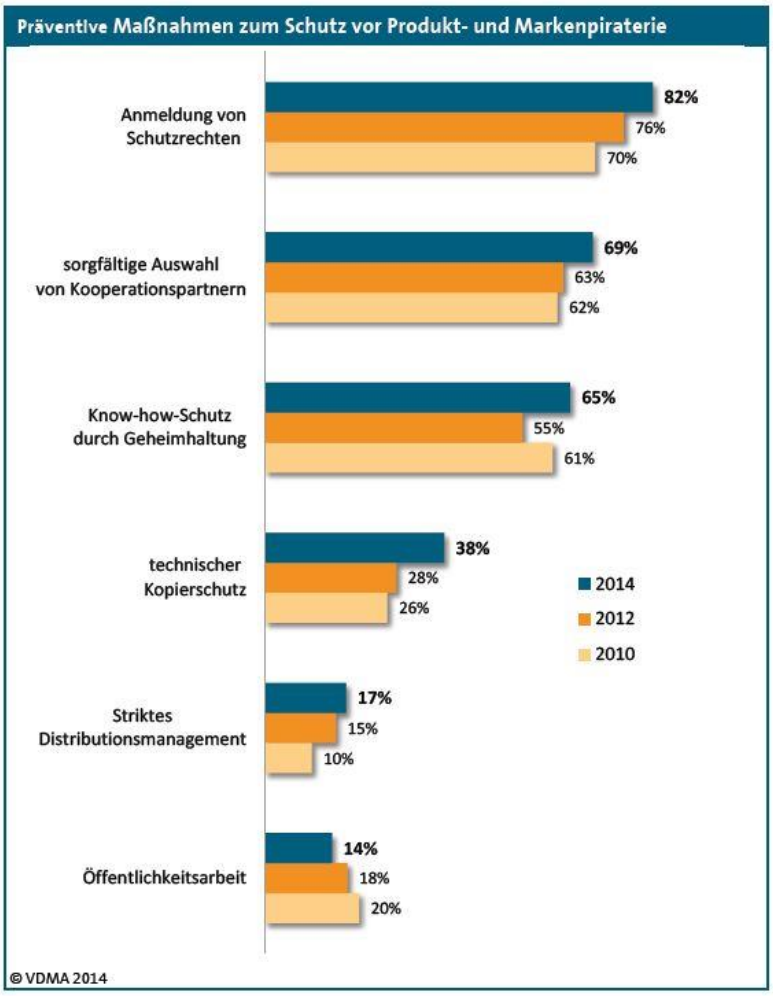

Abbildung 2: Präventive Maßnahmen zum Schutz vor Produkt- und Markenpiraterie (VDMA, 2014; S. 19).

Schaut man sich die Aufteilung der ergriffenen technischen Schutzmaßnahmen an, so stellt man fest, dass die am häufigsten ergriffene Maßnahme die Produktkennzeichnung darstellt, mit 30%. Jedoch ist hier auch ein Rückgang im Vergleich zum Jahr 2012 festzustellen (*siehe Abbildung 3*).

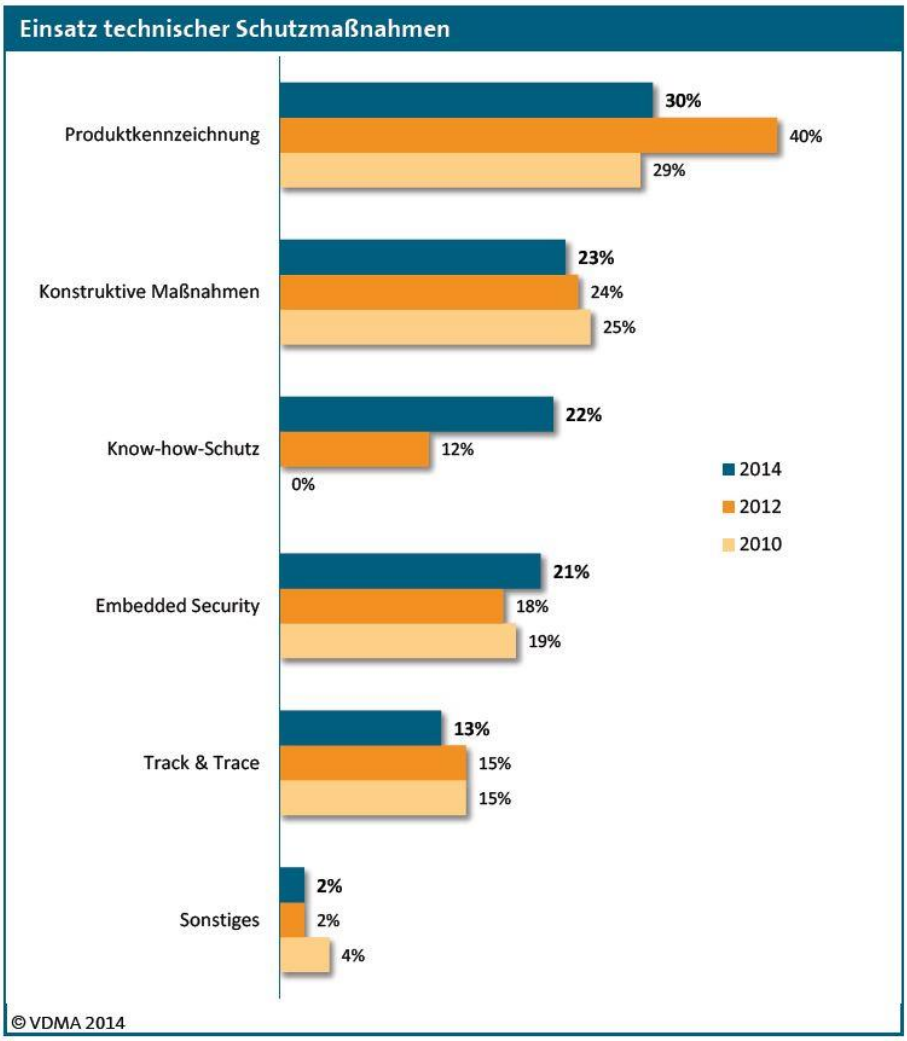

Abbildung 3: Einsatz technischer Schutzmaßnahmen (VDMA, 2014; S. 22).

Laut VDMA (2014) gaben ganze 18% der Unternehmen, die keine Maßnahmen umgesetzt haben, an, dass die Vielfalt an verfügbaren Maßnahmen zu umfangreich wäre. Fast ein Fünftel der Unternehmen die bisher auf den Einsatz von technischen Schutzmaßnahmen verzichtet haben, taten dies also aufgrund von fehlendem Know-How um die richtigen Maßnahmen auszuwählen oder aufgrund fehlender Entscheidungsfreude.

Insgesamt kann aus der neuen Studie gelesen werden, dass der Trend weiter anhält und Unternehmen auch in den kommenden Jahren weiterhin mit Produktpiraterie zu kämpfen haben.

Vor allem im Bereich der eingesetzten Maßnahmen gegen Produktpiraterie scheint noch großes Potential zu herrschen. Immer noch setzt ein Großteil der Unternehmen auf Schutzrechte, wobei gleichzeitig die Meinung überwiegt, dass die gesetzlichen Regelungen noch nicht ausreichend sind um effektiv und nachhaltig vor Produktpiraterie zu schützen (VDMA, 2014).

4 Überblick über technische Schutzmaßnahmen

Für diese Arbeit werden die in *Tabelle 1* aufgelisteten technischen Schutzmaßnahmen genauer erläutert. Diese Liste ist nicht abschließend, gibt aber einen guten Überblick über die bekannten und am weitesten verbreiteten technischen Schutzmaßnahmen gegen Produktpiraterie.

Wie in *Tabelle 1* zu sehen handelt es sich bei den hier dargestellten Technologien hauptsächlich um Kennzeichnungstechnologien. Laut VDMA (2014) handelt es sich bei 30% der eingesetzten technischen Schutzmaßnahmen um Produktkennzeichnungen; diese stellen somit den Großteil der in der Wirtschaft umgesetzten technischen Schutzmaßnahmen dar. Entsprechend soll auch der Schwerpunkt dieser Arbeit an dieser Stelle ansetzen.

Tabelle 1: Liste technischer Schutzmaßnahmen gegen Produktpiraterie (in Anlehnung an Stockenberger, Durchholz & Günthner, 2011; S. 5).

Unikatskennzeichen	
Codes mit Rauschmuster	2-D Barcode
Stochastische Schwankungen im Druckbild	RFID
Oberflächenauthentifizierung	Künstliche DNA
Originalitätskennzeichen	
Digitaldruck / Prepress-Druckmerkmale	Siebdruck / Prägen
Hologramme	Sicherheitsstreifen /-faden
Clusterfolie	Intagliodruck
Echtfarbenelemente	Kippfarbe
Thermoreaktive, thermochrome, thermische Farbe	Fotochrome Farbe
Farbcodes	IR-/ UV-Farbpigmente (Infrarotfarben)
Elektromagnetische Merkmale	Röntgenfluoreszenz
Sicherheitsanstanzung	*Grauer Hintergrund = verborgene Merkmale*

Die einzelnen Maßnahmen werden in den jeweiligen Unterkapiteln noch etwas genauer betrachtet und die markantesten Merkmale herausgefiltert. Eine Liste mit allen Schutzmaßnahmen und einer einheitlichen Tabelle zur Unterscheidung aller Details (unter anderem Kopiersicherheit und Robustheit) in Anlehnung an Günthner, et al. (2010), findet sich im Anhang (*Detailliste technischer Schutzmaßnahmen*) wieder.

Zur besseren Übersicht sind die folgenden Maßnahmen jeweils in Unikats- und Originalitätskennzeichen, sowie in jeweils sichtbare bzw. offene und verborgene Merkmale unterteilt bzw. kategorisiert.

4.1 Unikatskennzeichen

Zunächst sollen alle Maßnahmen hier aufgeführt werden, die als Unikatskennzeichnung dienen. Unikatskennzeichen sind dadurch gekennzeichnet, dass man nicht nur die Originalität des Produktes verifizieren kann, sondern auch jedes einzelne Produkt verifizieren kann. Oftmals sind diese Maßnahmen dadurch geprägt, dass eine Speicherung von Daten erfolgen kann (Abele, et al. 2011).

4.1.1 Offene Merkmale

Die folgenden Maßnahmen zeichnen sich durch offene Merkmale aus (*siehe Kapitel 5.1.1*).

4.1.1.1 Codes mit Rauschmuster (Copy Detection Pattern)

Kennzeichnungstyp: Unikatskennzeichen	
Kennzeichen	**Sichtbarkeit**
• Gedrucktes Rauschmuster	• Offenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Binäre Daten

Codes mit Rauschmuster, auch Copy Detection Pattern (CDP) genannt, sind zufällig erstellte Muster. Die Muster zeichnen sich durch extrem feine Details aus, welche aufgrund von Qualitätsverlust nicht exakt kopiert werden können. Bei der Erstellung des Merkmals wird das Muster zunächst gescannt und digital abgespeichert bzw. hinterlegt (Günthner, et al. 2010). Die Muster sind prinzipiell variable in Form, Farbe und Größe und können vom Kunden entsprechend ausgesucht werden. Die minimale Größe beträgt dabei ca. 12 mm² (Schreiner Group, ohne Datum).

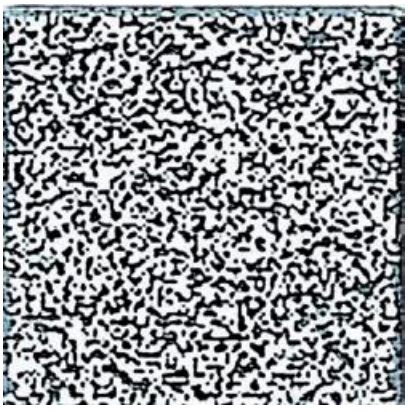

Abbildung 4: Copy Detection Pattern (Günthner, et al. 2010; S. 45).

Bereits bei der Erstaufbringung des Musters und dem ersten Scan kommt es zu einem Qualitätsverlust. Der Verlust der Qualität wird dabei gemessen und ergibt den sogenannten „Distanzwert“. Bei weiteren Scans wird anschließend das Bild mit dem digital hinterlegten Originalbild verglichen. Wird versucht das Rauschmuster zu kopieren oder zu fälschen, so verändert dies den zuvor kalibrierten „Distanzwert“ (INS, 2010).

Das Rauschmuster ermöglicht den Austausch von Nutzdaten (keine Steuer- / Protokolldaten) wobei die letztendliche Speicherkapazität von der Größe des Musters abhängt. Eine

Änderung der hinterlegten Informationen ist später nicht mehr möglich (Günthner, et al. 2010).

Das Muster ist prinzipiell leicht zu manipulieren bzw. zu zerstören. Ebenso muss bedacht werden, dass die Daten entsprechend gesichert werden um eine Auslesung der Informationen durch potentielle Fälscher verhindert werden kann. Wird das Originalbild, sowie der gemessene Distanzwert in Erfahrung gebracht ist es prinzipiell möglich das Merkmal zu fälschen. Typische Einsatzgebiete sind vor allem Banknoten und Dokumente (Günthner, et al. 2010).

4.1.1.2 2-D Barcode

Kennzeichnungstyp: Unikatskennzeichen	
Kennzeichen	**Sichtbarkeit**
• 2-D Barcode	• Offenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Ziffern und ASCII-Zeichen

Bei einem 2-D Barcode handelt es sich um eine „[o]ptoelektronisch lesbare Anordnung aus Punkten und Lücken (z.B. Matrixcode) in einem Raster“ (Günthner, et al. 2010; S.32). Das Muster selbst (*siehe Abbildung 5*) weist zwar Ähnlichkeiten mit dem des CDP auf (*siehe Abbildung 4*; S. 8), ist aber aufgrund seiner groben Ausführung bereits mit einfachsten Mitteln kopierbar.

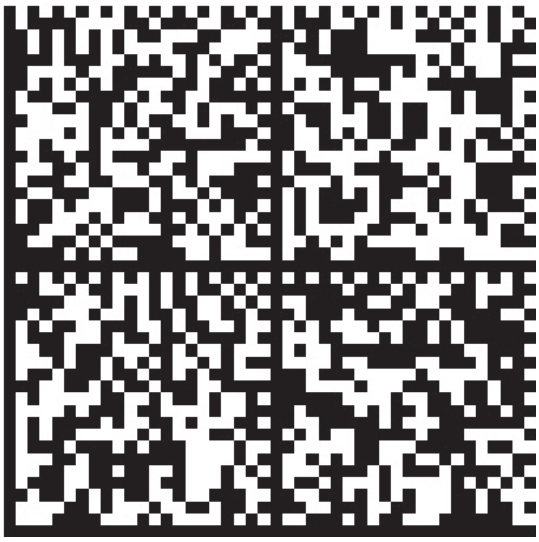

Abbildung 5: 2-D Barcode (Günthner, et al. 2010; S. 32).

Diese Maßnahme kommt hauptsächlich in der Logistik und bei Medikamenten zum Einsatz. Hierbei bietet es eine etwas sicherere Maßnahme als ein 1-D Barcode und erlaubt die Speicherung von Informationen (Günthner, et al. 2010).

4.1.1.3 Stochastische Schwankungen im Druckbild

Kennzeichnungstyp: Unikatskennzeichen	
Kennzeichen	**Sichtbarkeit**
• Merkmal entsteht im Druckprozess	• Offenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Keine

Bei dieser Methode werden Schwankungen in einem Druckbild erfasst und zum Zwecke der Produktkennzeichnung ausgenutzt. Vorhandene Schwankungen die beim Druckprozess zufällig entstanden sind werden erfasst und in eine Datenbank aufgenommen. Das Merkmal ist dabei aufgrund der nicht kalkulierbaren Schwankungen nicht reproduzierbar. Einzig die Übertragung muss gesichert werden, damit die Informationen zur Authentifizierung nicht abgefangen werden können. Diese Maßnahme wird typischerweise zur Markierung von Verpackungen verwendet (Günthner, et al. 2010).

4.1.2 Verborgene Merkmale

Die folgenden Maßnahmen sind dadurch geprägt, dass die Merkmale nicht offen sichtbar sind, sondern stattdessen verborgen vorliegen (*siehe Kapitel 5.1.1*).

4.1.2.1 RFID (Radiofrequenzidentifikation)

Kennzeichnungstyp: Unikatskennzeichen	
Kennzeichen	**Sichtbarkeit**
• RFID Transponder	• Verborgenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Elektromagnetisch	• Digitale Daten auf Mikrochip

Ein RFID Transponder besteht aus einem Mikrochip und einer integrierten Antenne. Über die Antenne eines externen Auslesegerätes wird Energie in Form eines (elektro-) magnetischen Feldes an die Antenne des Transponders übertragen. Damit kann der Mikrochip mit Energie versorgt werden um auf ihm enthalten Daten an das Auslesegerät zu senden. Somit entsteht die Möglichkeit zum Austausch von Binärdaten (Günthner, et al. 2010).

Die Standardgröße beträgt normalerweise ca. 4x4 cm und erlaubt die Speicherung von mehreren hundert Bit. Rein theoretisch erlaubt die Technologie eine Auslesung von bis zu 200 Tags pro Sekunde aus einer Entfernung von bis zu zehn Metern (INS, 2010). Nach dem Scan können die Informationen mit einer Datenbank abgeglichen werden, was eine

Identifikation des Produktes erlaubt. Hierbei ist es jedoch wichtig, dass die Informationen entsprechend verschlüsselt sein müssen (INS, 2010).

RFID Transponder werden hauptsächlich in der Logistik eingesetzt. Durch Einsatz von speziellen Informationen die auf den Tag gespeichert werden, können diese auch zum Zwecke der Produktkennzeichnung eingesetzt werden (Günthner, et al. 2010).

4.1.2.2 Oberflächenauthentifizierung (Laseroberflächenauthentifizierung)

Kennzeichnungstyp: Unikatskennzeichen	
Kennzeichen	**Sichtbarkeit**
• Oberflächenstruktur	• Verborgenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Keine (Ausnahmen möglich)

Nach Günthner, et al. (2010) wird das Prinzip der Oberflächenauthentifizierung erläutert als „Reflexion eines auf eine Oberfläche treffenden Laserstrahls wird von mehreren Scannern erfasst, woraus sich ein spezifisches mikroskopisches Bild ergibt“. Anhand dieser Reflexionen entsteht für jede Oberfläche ein individuelles, nicht kopierbares Bild (Günthner, et al. 2010). Es entsteht eine Art Fingerabdruck. Diese Maßnahme eignet sich besonders für Werkstücke, bei denen eine Etikettierung oder das Aufbringen von Codes keine Lösung darstellt (INS, 2010).

Ähnlich wie bei anderen Maßnahmen müssen die erfassten Daten der Scanner wieder in einer Datenbank hinterlegt werden um spätere Scans abgleichen zu können. Sofern die Stelle der Prüfung bekannt ist, können Manipulationen an der entsprechenden Oberfläche durchgeführt werden um spätere Scans zu verfälschen. Auch die Robustheit kann je nach Werkstoff variieren. Die Maßnahme findet vor allem Anklang bei Verpackungen, Papier-, Metall- und Kunststoffoberflächen (Günthner, et al. 2010).

4.1.2.3 Künstliche DNA

Kennzeichnungstyp:	
Kennzeichen	**Sichtbarkeit**
• Künstliche DANN / Mikrocodes	• Verborgenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch, physikalisch	• DNA, Text/ Code

Bei der künstlichen DNA handelt es sich um eine Methode, bei der künstlich hergestellte DNA produziert wird und auf ein Produkt aufgetragen wird. Die Authentifizierung kann auf

verschiedenen Wegen erfolgen. Zum einen kann die DNA bereits mit Hilfe einer UV-Lampe sichtbar gemacht werden. Jedoch kann auf diese Weise noch keine eindeutige Zuordnung erfolgen. Mit Hilfe eines Mikroskops können kleine Mikrocodes sichtbar gemacht werden, die mit der DNA aufgetragen werden. Diese sind einmalig und können in einer Datenbank dem Produkt zugeordnet werden (SDNA Technology GmbH, ohne Datum).

Die DNA ist grundsätzlich sehr schwer zu kopieren, da eine Reproduzierung der DNA sehr aufwendig ist. Jedoch kann die DNA sehr leicht abgewischt werden und ist auch anfällig gegen Umwelteinflüsse. Grundsätzlich solle sie geschützt angebracht werden. Je nach Anwendung müssen demnach verschiedene Ausprägungen genutzt werden (SDNA Technology GmbH, ohne Datum).

4.2 Originalitätskennzeichen

Im Gegensatz zu den Unikatskennzeichen können bei sog. Originalitätskennzeichnen keine Rückschlüsse auf das individuelle Produkt gemacht werden. Es kann allerdings die Originalität des Produktes nachgewiesen werden, sodass ein Unternehmen feststellen kann, ob ein Produkt von ihnen stammt oder nicht (Abele, et al. 2011).

4.2.1 Offene Merkmale

Auch in dieser Kategorie sollen zunächst die Maßnahmen mit offenen Merkmalen aufgelistet werden (*siehe Kapitel 5.1.1*).

4.2.1.1 Digitaldruck / Prepress-Druckmerkmale (Digitales Wasserzeichen)

Kennzeichnungstyp: Originalitätskennzeichen	
Kennzeichen	**Sichtbarkeit**
• Feine Muster	• Offenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Keine (außer Mikrotext)

Es gibt verschiedene Arten und Ausprägungen des Digitaldrucks. Zum einen gibt es den sogenannten Guillochendruck, das digitale Wasserzeichen und den Mikrotext (Günthner, et al. 2010).

Beim Guillochendruck handelt es sich um sehr feine und sehr komplexe Muster (*siehe Abbildung 6*). Die Muster setzen sich aus ununterbrochenen, eng nebeneinander liegenden Linien zusammen, die in sich verschlungen sind und nach geometrischen Gesetzmäßigkeiten

angeordnet wurden. Dabei verhindert die sehr feine Struktur ein Kopieren der Muster (Günthner, et al. 2010; INS, 2010).

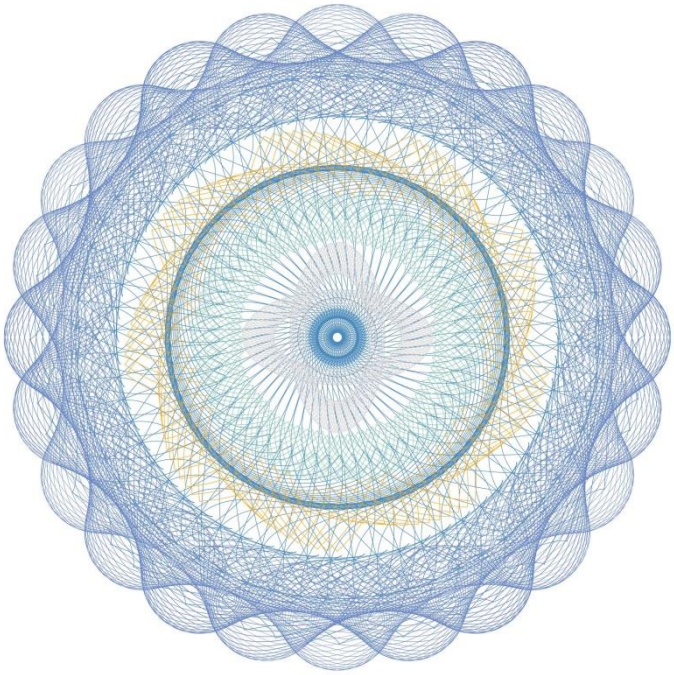

Abbildung 6: Guillochendruck (highendwathces.com, ohne Datum).

Beim digitalen Wasserzeichen werden noch vor dem Drucken, nämlich während der Druckvorstufe, Softwareseitig Merkmale mit eingebunden. Diese Merkmale sind dann später als Informationen im Druckbild enthalten. Diese Änderungen des Druckbildes sind für das menschliche Auge unsichtbar und können auch nicht kopiert werden. Mit Hilfe eines kleinen, transparenten Filters können die Informationen sichtbar gemacht werden. Auch die Verwendung von Scannern zur Verifikation ist möglich (INS, 2010).

Die dritte Ausprägung, Mikrotexte, sind Schrifthöhen von weniger als 0,33 mm. Auch hier ist eine Kopie nur sehr schwer zu erstellen. Im Gegensatz zu den ersten beiden Ausprägungen lassen sich beim Mikrotext Daten im Sinne von Text hinterlegen (Günthner, et al. 2010).

Typischerweise werden diese Schutzmaßnahmen vorwiegend für Wertpapiere, Dokumente und Ausweise verwendet (Günthner, et al. 2010).

4.2.1.2 Siebdruck / Prägen

Kennzeichnungstyp:	**Originalitätskennzeichen**
Kennzeichen	**Sichtbarkeit**
• Fühlbarer Schriftzug	• Offenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch, haptisch	• Schrift, Muster

Ähnlich wie beim Intagliodruck handelt es sich beim Siebdruck um einen fühlbaren Schriftzug. Hierbei wird ein Bedruckstoff mithilfe eines Siebes bedruckt. Die Farbe wird mit Hilfe einer sogenannten Rakel durch ein Sieb auf den Bedruckstoff gepresst. Dabei können relativ hohe Farbschichten erzeugt werden, anders als bei anderen Druckmethoden (Günthner, et al. 2010).

Nachteil ist die freie Verfügbarkeit der Technologie. Jedoch ist sie robust gegen chemische und mechanische Beanspruchung. Es wird hauptsächlich als Folienaufdruck verwendet (Günthner, et al. 2010).

4.2.1.3 Hologramme (Optically Variable Device)

Kennzeichnungstyp:	**Originalitätskennzeichen**
Kennzeichen	**Sichtbarkeit**
• Hologramm (-folie)	• Offenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Keine (Ausnahme möglich)

Eine der am markantesten auffallenden und am weitesten verbreitete technische Schutzmaßnahme, die vermutlich jeder schon einmal gesehen hat, ist das Hologramm (INS, 2010). Meistens auf dem Etikett oder auf der Verpackung angebracht handelt es sich hierbei um ein offenes Merkmal, das vom Kunden direkt wahrgenommen und auch überprüft werden kann (Günthner, et al. 2010). Dieses Merkmal kennen viele nicht nur von Textilien, sondern man findet es auch wieder auf Geldscheinen.

Für die genaue Überprüfung und Verifizierung des Merkmals werden jedoch ggf. Mikroskope und eine gute Beleuchtung benötigt. Durch eine genaue Überprüfung und durch Verwendung komplexer Ausführungen ist die Reproduzierung dieser Merkmale sehr komplex. Jedoch haben sich bereits einige Produktpiraten auf die Fälschung von Hologrammen spezialisiert, weshalb die Komplexität durch Ergänzen weiterer Merkmale ständig erhöht wird (INS, 2010).

4.2.1.4 Sicherheitsstreifen /-faden

Kennzeichnungstyp:	**Originalitätskennzeichen**
Kennzeichen	**Sichtbarkeit**
• Metallischer Faden	• Offenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Keine

Sicherheitsfäden können bei der Herstellung in den Bedruckstoff integriert werden. Dieser Faden kann mit einem sichtbaren oder unsichtbaren Text versehen werden. Zur Authentifizierung wird dieser Text ausgelesen. Die Maßnahme ist schwer zu kopieren und kommt vor allem bei Banknoten und bei Dokumenten zum Einsatz (Günthner, et al. 2010).

4.2.1.5 Clusterfolie

Kennzeichnungstyp:	**Originalitätskennzeichen**
Kennzeichen	**Sichtbarkeit**
• Folie mit Farbkippeffekt	• Offenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Keine

Bei der Clusterfolie handelt es sich um eine hochglänzende Folie aus Nano-Cluster-Schichten. Diese Folie ist bereits mit dem menschlichen Auge erkennbar und erzeugt Farbkippeffekte. Je nach Blickwinkel ändern sich die Farben der Folie (Günthner, et al. 2010).

Die Maßnahme ist durch eine hohe Kopiersicherheit charakterisiert, wobei eine Manipulation durch mechanische Zerstörung der Folie möglich ist. Typisches Einsatzgebiet sind vor allem Verpackungen (Günthner, et al. 2010).

4.2.1.6 Intagliodruck (Stichtiefdruck)

Kennzeichnungstyp:	**Originalitätskennzeichen**
Kennzeichen	**Sichtbarkeit**
• Druckbild aus dickflüssiger Farbe	• Offenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch, haptisch	• Text

Beim Intagliodruck, auch Stichtiefdruck genannt, handelt es sich um eine spezielle Drucktechnik bei der ein fühlbares Oberflächenmuster erzeugt wird. Hierzu ist eine spezielle Drucktechnik nötig, die das Kopieren der Maßnahme erschwert. Zum Einsatz kommt dieses Verfahren vor allem bei Banknoten, Pässen und Urkunden (Günthner, et al. 2010).

4.2.1.7 Echtfarbenelemente

Kennzeichnungstyp:	**Originalitätskennzeichen**
Kennzeichen	**Sichtbarkeit**
• Farbpigmente außerhalb der üblichen rgb/cmyk-Werte	• Offenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Keine

Echtfarbelemente zeichnen sich durch eine besonders hohe Leuchtkraft der Farbpartikel aus, wodurch eine Reproduzierung mit normalen Kopierern und Druckern nicht erreicht werden kann. Die Echtfarbenelemente kommen vor allem im Bereich von Fahrkarten, Eintrittskarten und (Flug-) Tickets zum Einsatz (Günthner, et al. 2010).

4.2.1.8 Kippfarbe (Optisch variable Farben)

Kennzeichnungstyp: Originalitätskennzeichen	
Kennzeichen	**Sichtbarkeit**
• Pigmente mit Farbkippeffekt	• Offenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Keine

Ähnlich wie bei der Clusterfolie kommen hier Farbpigmente zum Einsatz, die je nach Betrachtungswinkel des Auges und Lichteinfall die Farben ändern. Die Kopiersicherheit kann hierbei wiederum stark variieren da die Farben teilweise frei erwerblich sind (Günthner, et al. 2010). Ein typisches Kopieren des Merkmales ist jedoch nicht möglich (INS, 2010).
Einsatzgebiete sind vor allem Geldscheine, Verpackungen, Dokumente und Medikamente (Günthner, et al. 2010).

4.2.1.9 Thermoreaktive, thermochrome, thermische Farbe

Kennzeichnungstyp: Originalitätskennzeichen	
Kennzeichen	**Sichtbarkeit**
• Thermoreaktive Farbpigmente	• Offenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Thermisch	• Keine (Ausnahmen möglich)

Bei der thermoreaktiven Farbe handelt es sich um wärmeempfindliche Farben, die ihre Farbe aufgrund von thermischen Einflüssen ändern. Dabei können grundsätzlich zwei Merkmale unterschieden werden. Bei der thermochromen bzw. thermoreaktiver Farbe ist die Farbänderung reversibel und nachdem wieder die Ausgangstemperatur erreicht wird stellt sich auch wieder die Originalfarbe ein. Somit können mehrere Authentifizierungsprozesse unternommen werden. Bei der thermischen Farbe ist die Farbänderung irreversibel (Günthner, et al. 2010).
Grundsätzlich ist eine Farbtonänderung als auch ein Farbumschlag möglich. Allerdings sind die Farben frei erhältlich, was das Kopieren vereinfacht. Durch zusätzliche Lackierungen

kann die Robustheit der Maßnahme erhöht werden. Zu finden ist diese Maßnahme meist bei Verpackungen und Etiketten (Günthner, et al. 2010).

4.2.2 Verborgene Merkmale

Folgende Maßnahmen weisen verborgene Merkmale auf (*siehe Kapitel 5.1.1*).

4.2.2.1 Fotochrome Farbe

Kennzeichnungstyp:	**Originalitätskennzeichen**
Kennzeichen	**Sichtbarkeit**
• Photochrome Farbpartikel	• Offenes/ verborgenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Keine

Bei fotochromen Farben handelt es sich um Farben, die abhängig von der Beleuchtung ihre Farbe ändern können. Je nachdem ob Tages-/ oder Kunstlicht benutzt wird um die Farbe zu beleuchten entstehen unterschiedliche Farben. Dies hängt mit dem UV-Anteil von Tages-/ und Kunstlicht zusammen. Je nach Intensität und spektralem Zusammensetzung des UV-Anteils des Lichts können die resultierenden Farben variieren. Eine Kopie der Maßnahme ist nur unter Verwendung der korrekten fotochromen Farben im richtigen Verhältnis möglich (Günthner, et al. 2010).

4.2.2.2 Farbcodes (Mikrofarbcodes)

Kennzeichnungstyp:	**Originalitätskennzeichen**
Kennzeichen	**Sichtbarkeit**
• 5-45 µm kleine Partikel aus Melanin-Alkyd-Polymer	• Verborgenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Keine

Mikrofarbcodes bestehen aus winzig kleinen Kunststoffpartikeln, die sich wiederum aus winzig kleinen Farbschichten zusammensetzen. Je nach Anordnung dieser Farbschichten entsteht ein bestimmter Code. Dieser Code kann zur Verifikation genutzt werden und ist für das menschliche Auge unsichtbar (Günthner, et al. 2010). Die zwischen 5-45 µm großen Partikel setzen sich aus 4-10 Farbschichten zu je ca. 1 µm zusammen. Insgesamt können hierbei über vier Milliarden Basis-Farbcodes erstellt werden. Zusätzlich können fluoreszierende und magnetische Schichten hinzugefügt werden, was die Kopiersicherheit um ein vielfaches erhöht. Diese Maßnahme kann sowohl während des

Herstellungsprozesses, als auch zu einem späteren Zeitpunkt hinzugefügt werden (INS, 2010).

Die Maßnahme zeichnet sich durch eine sehr hohe Kopiersicherheit aus da es nur sehr wenige Anbieter für diese Technologie gibt. Gleichzeitig weist sie eine hohe Manipulationssicherheit und Robustheit auf (Günthner, et al. 2010).

Einsatzgebiet sind vor allem Etiketten, Siegel und Spritzguss (Günthner, et al. 2010).

4.2.2.3 IR-/ UV-Farbpigmente (Infrarotfarben)

Kennzeichnungstyp:	**Originalitätskennzeichen**
Kennzeichen	**Sichtbarkeit**
• Farbpigmente	• Verborgenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Keine

Diese Maßnahme funktioniert nach dem Lumineszenz-Prinzip. Werden IR-/UV-Farbpigmente mit IR-/ UV-Licht angeregt, so emittieren diese Licht einer spezifischen Wellenlänge. Erst durch diese Anregung mit Licht werden die Farbpigmente für das menschliche Auge bzw. für spezifische Lesegeräte sichtbar (INS, 2010).

Die Wellenlänge kann je nach Bedarf variieren. Auch kann die Auslesung entsprechend angepasst werden. Ist die bloße Wahrnehmung für das menschliche Auge nicht ausreichend, so können Wellenlängen gewählt werden die anschließend von spezifischen Lesegeräten ausgelesen werden. Dabei kommen Laser zum Einsatz mit integrierter Sensorik, die die emittierte Wellenlänge erfassen und mit den hinterlegten Daten abgleichen (INS, 2010).

Der Kopierschutz kann bei dieser Maßnahme je nach gewählter Ausführung stark variieren. So sind beispielsweise einige dieser IR-/UV-Farben frei zugänglich, was ein Kopieren sehr einfach möglich macht. Ebenso können die Farben mechanisch entfernt werden, was eine Manipulation möglich macht (Günthner, et al. 2010).

Ein typisches Einsatzgebiet sind vor allem Banknoten und Medikamente (Günthner, et al. 2010).

4.2.2.4 Elektromagnetische Merkmale

Kennzeichnungstyp:	**Originalitätskennzeichen**
Kennzeichen	**Sichtbarkeit**
• Micro-Sicherheitsfaden	• Verborgenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Elektromagnetisch	• Keine

Das Prinzip der elektromagnetischen Merkmale basiert auf einem amorphem Metall (weisen keine kristalline Struktur auf, sind aber dennoch leitfähig) welches als Mikrosicherheitsfaden von Glasummantelt wird. Dabei weist das Metall eine bestimmte Kennung auf. Mit Hilfe spezieller Legierungen und physikalischer Behandlungen können elektromagnetische Eigenschaften erzeugt werden. Diese Eigenschaften werden später anhand eines elektromagnetischer Scanners ausgelesen (Günthner, et al. 2010).

Die elektromagnetischen Eigenschaften sind dabei kaum rekonstruierbar und auch nur sehr schwer zu entfernen. Allerdings muss auch hier die Übertragung gesichert werden, damit die Merkmale nicht abgefangen werden können. Diese Maßnahme findet sich vor allem bei Ersatzteilen, Bekleidung, Dokumente, Chip- und Kreditkarten wieder (Günthner, et al. 2010).

4.2.2.5 Röntgenfluoreszenz

Kennzeichnungstyp:	**Originalitätskennzeichen**
Kennzeichen	**Sichtbarkeit**
• Zusätzliches Markierungselement	• Verborgenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Elektromagnetisch, physikalisch	• Keine

Bei dieser Sicherheitsmaßnahme kommt die Röntgenfluoreszensspektroskopie zum Einsatz zur Bestimmung der qualitativen und quantitativen Zusammensetzung einer Probe. Diese Probe ist ein zusätzliches Markierungselement, dass dem Produkt beigemischt wurde. Die Röntgenfluoreszensspektroskopie gibt eindeutige Merkmale des Markierungselementes wieder. Diese können kaum gefälscht werden, was eine hohe Sicherheit der Maßnahme zur Folge hat. Ebenfalls ist die Maßnahme sehr robust gegenüber äußeren Einflüssen (Günthner, et al. 2010).

Jedoch ist hier ein relativ großer Aufwand von Nöten um die Authentifizierung durchzuführen.

4.2.2.6 Sicherheitsanstanzung

Kennzeichnungstyp:	**Originalitätskennzeichen**
Kennzeichen	**Sichtbarkeit**
• Markierung am Verpackungskarton	• Verborgenes Merkmal
Authentifizierungsmöglichkeiten	**Speichermöglichkeiten**
• Optisch	• Keine

So simpel wie diese Maßnahme ist, so einfach kann man sie theoretisch auch kopieren. Es handelt sich bei der Sicherheitsanstanzung um ein Verfahren, bei dem willentlich ein Stück des Verpackung Kartons stehen gelassen wird, obwohl dies nicht nötig wäre. Dieses bewusste Stehenlassen soll den Eindruck eines Fehlers erwecken (Günthner, et al. 2010). Wird das Produkt nun kopiert, so wird dieser mutmaßliche Fehler nicht mitkopiert. Wird nun die Verpackung auf das überstehende Teil untersucht kann eine Authentifizierung durchgeführt werden. Der Nachteil dieser Methode liegt darin, dass sie sehr einfach kopiert werden kann. Ausschlaggebend ist, dass das Wissen über die Maßnahme nicht nach außen dringt. Sobald bekannt ist, dass es sich um ein gewolltes Stehenlassen handelt, kann die Maßnahme ohne großen Aufwand kopiert werden (Günthner, et al. 2010).

5 Auswahl geeigneter Schutzmaßnahmen

Wie in *Kapitel 4* vorgestellt, haben die verschiedenen technischen Schutzmaßnahmen verschiedene Eigenschaften und Merkmale anhand derer diese klassifiziert werden können. Gemäß diesen Merkmalen können verschiedene Maßnahmen identifiziert werden. Je nach gesetztem Schutzziel und anderen Anforderungen können verschiedene Maßnahmen ausgewählt werden. Hierbei ist es vor allem wichtig zu wissen, welche Anforderungen an die Maßnahme gestellt sind bzw. welches Ziel erreicht werden soll.
Technische Schutzmaßnahmen können sehr kostenintensiv sein, weshalb sich vor allem auch kleinere Unternehmen oftmals gegen den Einsatz dieser Maßnahmen entscheiden (VDMA, 2014). Umso wichtiger ist die Auswahl der richtigen Schutzmaßnahme für das individuelle Produkt. Nicht immer ist es notwendig die aufwendigste und teuerste Maßnahme umzusetzen und je nach Anforderung kann auch eine wirtschaftlichere Lösung zum Ziel führen.

In diesem Kapitel soll deshalb ein kleiner Überblick darüber gegeben werden, wie man die „richtige“ Maßnahme identifiziert. Des Weiteren soll ebenfalls auf eine besondere Form technischer Schutzmaßnahmen eingegangen werden, nämlich dem sogenannten „Track & Tracing“.

5.1 Anforderungen identifizieren

Grundsätzlich lassen sich technische Schutzmaßnahmen in vielerlei Kategorien einteilen und auch unterteilen. Im Folgenden soll eine Auswahl, der dem Verfasser als wichtigsten Anforderungen erscheinenden Merkmale, etwas näher beschrieben werden. Anhand dieser Merkmale lassen sich die in *Kapitel 4* vorgestellten Schutzmaßnahmen logisch unterteilen und verschiedene Maßnahmen für verschiedene Anwendungszwecke isolieren.

5.1.1 Sichtbarkeit der Merkmale

Die wohl offensichtlichste Anforderung ist die Sichtbarkeit des Merkmals. Die vorgestellten Merkmale können entweder für jedermann sichtbar am Produkt angebracht werden, oder man kann es an einer verborgenen Stelle anbringen.

Dies kann verschiedene Gründe haben. Ein offenes Merkmal kann zum einen auch vom Endkunden überprüft werden, was den Prüfaufwand allgemein verringert, und somit vom Kunden eine Verifizierung erfolgt. Jedoch können Kunden oftmals ein gefälschtes Merkmal nur schwer von einem originalen unterscheiden (INS, 2010).
Andererseits ist das Merkmal auch für mögliche Fälscher offen erkennbar. Dies erleichtert zwar nicht den eigentlichen Fälschungsprozess der Maßnahme, allerdings entfällt das Suchen nach verdeckten Merkmalen, was den Kopiervorgang beschleunigen könnte.
Umgekehrt sieht es bei den verdeckten Merkmalen aus. Zum einen kann vom Endkunden nicht mehr direkt überprüft werden, ob es sich um ein Original handelt und der Prüfungsprozess ist im Normalfall etwas aufwendiger. Dafür ist es schwieriger für Fälscher die Maßnahme zu kopieren, da diese erst einmal gefunden werden muss.

Je nach Anwendungszweck muss also entschieden werden, ob ein offenes oder verborgenes Merkmal benötigt wird. Gerade im Bereich von Textilien ist oftmals gewünscht, dass ein durch den Kunden einsehbares Merkmal gewählt wird.

5.1.2 Speichermöglichkeiten

Ein anderes wichtiges Merkmal ist die Speichermöglichkeit der Maßnahmen. Je nach Anwendungszweck kann es gefordert sein, dass zusätzliche Informationen gespeichert werden sollen. Somit kann aus einem Originalitätskennzeichen ein Unikatskennzeichen werden. Mit Hilfe dieser Informationen können bestimmte Details über das Produkt gespeichert und später abgerufen werden. Somit lässt sich jedes Produkt individuell identifizieren, was ein Fälschen des Produktes erschwert. Dies kann vor allem bei komplexeren Produkten oder Anlagenteilen gefordert sein (Günthner, et al. 2010).
Für andere Produkte ist dies eventuell nicht von Bedeutung und die Implementierung eines Originalitätskennzeichens ist ausreichend. Somit kann auf kostenintensive Maßnahmen mit Speichermöglichkeiten verzichtet werden.

5.1.3 Authentifizierungsmöglichkeiten

Die Authentifizierung von technischen Schutzmaßnahmen kann auf mehreren Wegen erfolgen. Wie in *Tabelle 2* (Anhang: *Detailliste technischer Schutzmaßnahmen*) zu sehen, gibt es verschiedene Kriterien zur Authentifizierung.
Unterschieden werden können die folgenden Merkmale:

- Lese-/ Prüfgerät oder direkt durch Menschen ausgelesen
- Optisches vs. haptisches vs. thermisches vs. elektromagnetisches Wirkprinzip
- Mit oder ohne Berührung bei der Prüfung

Jede der Merkmale hat dabei ihre Vor- und Nachteile. Wohingegen der Einsatz von Prüfgeräten meist mit einer genaueren Prüfung verbunden ist, so weisen Maßnahmen, die ohne die Hilfe von Lese- und Prüfgeräten ausgelesen werden können, oftmals eine geringere Fälschungssicherheit auf. Allerdings ist die Prüfung mit Hilfsmittels meist komplizierter und muss in geeigneter Weise kommuniziert werden (Günthner, et al. 2010).
Merkmale die keiner Hilfsmittel bedürfen können zusätzlich auch vom Endverbraucher überprüft werden (sofern keine Einweisung erforderlich ist), was die Awareness auch bei Kunden erhöhen kann.
Ähnlich verhält es sich mit dem Wirkprinzip und der berührenden bzw. berührungslosen Prüfung. Je nach Anforderung kann eines der Merkmale bevorzugt werden. Für welche Merkmale man sich letztendlich entscheidet hängt jedoch von allerlei Faktoren ab. Je nach Budget, gewünschtem Prüfaufwand und der Manipulationssicherheit bzw. Robustheit muss das Merkmal ausgesucht werden.

5.2 Track & Tracing

Eine weitere Anforderung an die technische Schutzmaßnahme kann das sogenannte Track & Tracing sein. Track & Tracing beschreibt ein Verfahren, das es erlaubt, den Verlauf eines Produktes in einer Logistikkette nachzuvollziehen.
Zusätzlich zu vorhandenen Unikatskennzeichen können an verschiedenen Stellen in der Logistikkette Daten nicht nur ausgelesen, sondern auch geschrieben werden. Dadurch entstehen eine Art Bewegungsdaten (Abele, et al. 2011). Vor allem bei Maßnahmen, die eine Speicherung von Daten erlauben und die mit Hilfe technischer Systeme ausgelesen werden können (z.B.: RFID, CDP) kommt dieses Verfahren zum Einsatz. An verschiedenen Stellen der Logistikkette können so Einzelheiten über den Verbleib des Produktes inkl. Datumsangaben gemacht werden. Wird ein Produkt gefälscht, so kann durch Auslesen der Bewegungsdaten erkannt werden, ob ein Produkt wirklich vom Hersteller kommt oder später in die Logistikkette eingeschleust wurde (Abele, et al. 2011). Track & Tracing ist vor allem interessant, um die Liefer-/ Logistikkette zu überwachen und sicherzustellen, dass die Produkte tatsächlich vom besagten Hersteller kommen.

6 Ausblick

Unternehmen werden vermutlich auch in Zukunft Probleme mit Produktpiraterie haben. Das Problem ist jedoch bekannt und es gibt bereits einige Strategien um sich zu wehren. Wie effektiv diese Strategien letztendlich sind wird sich in den kommenden Jahren zeigen.
Auch technische Schutzmaßnahmen tragen sicherlich zur Bekämpfung der Produktpiraterie bei. Wie in den vorherigen Kapiteln gesehen gibt es die verschiedensten Maßnahmen mit den verschiedensten Merkmalen. Für fast alle Anwendungsbereiche sollte sich auch eine technische Maßnahme finden lassen. Absolut kopiersicher sind jedoch die wenigsten der Maßnahmen.
Vor allem bei der Produktkennzeichnung ist der Einsatz von technischen Maßnahmen verbreitet. Sie sind und werden auch in Zukunft weiterhin einen wesentlichen Anteil am Kampf gegen Produktpiraterie haben. Dabei ist anzunehmen, dass auch vermehrt Maßnahmen mit Speichermöglichkeiten (Unikatskennzeichen) zum Einsatz kommen werden. Durch die stetige Weiterentwicklung der Technik werden vermutlich auch immer wieder neue Systeme zum Einsatz kommen die noch sicherer sind.

Einen absoluten Schutz gegen die Produktpiraterie können sie aber nicht liefern. Es sollten wohl weiterhin auch komplexe Strategien entwickelt werden, um nicht nur an einer Stelle Maßnahmen zu ergreifen. Auch auf organisatorischer Ebene und durch Analyse von Prozessabläufen sollten Maßnahmen entwickelt werden um die Fälschung von Produkten zu verhindern oder zu erschweren.

Literaturverzeichnis

Abele, E., Kuske, P., Lang, H. (2011). *Schutz vor Produktpiraterie*. [Ein Handbuch für den Maschinen und Anlagenbau]. Berlin, Heidelberg: Springer Verlag.

Günthner, W.A., Durchholz, J., Stockenberger, D., Wildemann, H., Pommer, P., Tschöke, T., et al. (2010). *Leitfaden zum Schutz vor Produktpiraterie durch Bauteilkennzeichnung.* Integrierter Produktpirateriesschutz durch Kennzeichnung und Authentifizierung kritischer Bauteile im Maschinen - und Anlagenbau. [Lehrstuhl für Fördertechnik Materialfluss Logistik (FML)].

Innovation mit Normen und Standards [INS]. (2010, 6. Dezember). *Integratives System zur einheitlichen Kennzeichnung und Identifizierung von Maschinenbauprodukten.* [NA 060 Normenausschuss Maschinenbau].

Schreiner Group GmbH & Co. KG. (ohne Datum). Echtheitsnachweis mit System. [Homepage des Herstellers]. Zugriff am 9. Dezember 2015 unter http://www.schreiner-bitsecure.com/0/systemintegration/

SDNA Technology GmbH. (ohne Datum). SelectaDNA / Künstliche DANN. [Homepage des Herstellers]. Zugriff am 12. Dezember 2015 unter http://www.selectadna.de/

Staake, T. Fleisch, E. (2008). *Countering Counterfeit Trade*. [Illicit Market Insights, Best-Practice Strategies, and Management Toolbox]. Berlin, Heidelberg: Springer-Verlag.

Stockenberger, D., Durchholz, J., Günthner, W.A. (2011). *Integrierte Sicherheitsmerkmale als Schutz vor Produktpiraterie im Maschinen- und Anlagenbau*. [Logistics Journal: Not reviewed publications].

Verband Deutscher Maschinen- und Anlagenbau e.V. [VDMA] (2012). *VDMA Studie Produktpiraterie 2012.* [VDMA Arbeitsgemeinschaft Produkt- und Know-how-Schutz].

Verband Deutscher Maschinen- und Anlagenbau e.V. [VDMA] (2014). *VDMA Studie Produktpiraterie 2014.* [VDMA Arbeitsgemeinschaft Produkt- und Know-how-Schutz].

Anhang

Detailliste technischer Schutzmaßnahmen

Tabelle 2: Detailliste technischer Schutzmaßnahmen (erstellt von dem Verfasser in Anlehnung an Günthner, et al. 2010).

Technische Schutzmaßnahmen															
Schutzmaßnahme		Kennzeichnungstypen			Kennzeichen	Materialien		Ort	Kennzeichnung/Applikation	Authentifizierung				Kontakt bei Prüfung	
Bezeichnung	Alt. Bezeich.	Originalitäts-	Identitäts-	Unikats-		Trägermaterial	Grundmaterial			Prüfung/Identifizierung	Tech. Gerät notwendig	Prüfhäufigkeit	Wirkprinzip der Prüfung	Berührend	Nicht Berührend
Codes mit Rauschmuster	Copy Detetion Pattern			x	Gedrucktes Rauschmuster	Bedruckbare Materialien	• Wie Trägermaterial • beliebig bei Etikett	• Produkt • Verpackung	• Direkt Bedrucken • Aufbringen eines Etiketts • Laserbeschriftung	Scanner, spezielles Lesegerät	x	Unbegrenzt	Optisch		x
2-D Barcode			x		2D-Barcode	Alle bedruckbaren Materialien	• Wie Trägermaterial • beliebig bei Etikett	Beliebig	• Drucken • laserbeschriftung • etc.	2D-Barcode-Scanner	x	Unbegrenzt	Optisch		x
Stochastische Schwankungen im Druckbild				x	Merkmal entsteht im Druckprozess	Alle bedruckbaren Materialien	• Wie Trägermaterial • beliebig bei Etiketten	• Produkt • Verpackung • Etikett	Druckmaschine	Spezielle Prüfgeräte, teilweise sind Handykameras etc. ausreichend.	x	Unbegrenzt	Optisch		x
RFID				x	IC mit Antenne zur (elektro)magnetischen Kopplung (Transponder)	Verschiedenste Formen (Label, Hard-Tag, etc.)	Frequenzabhängig (Schwierigkeiten bei leitfähigen Materialien)	• Als Etikett auf Produkt oder Verpackung • integriert • etc.	• Aufkleben • Eingießen • etc.	Antenne, Lesegerät, Rechner/Steuerung	x	Unbegrenzt	Elektro-magnetisch		x
Oberflächen-authentifizierung	Laser-oberflächen-authentifi-zierung			x	Oberflächenstruktur	Nicht notwendig	Alle nicht spiegelnden Materialien wie Papier, Pappe, Kartonagen, Kunststoff und bearbeitete Metalle	Definierte Stelle der (Bauteil-)Oberfläche	Mikroskopische Aufnahme mit optischen Sensoren	Mikroskopische Aufnahme mit optischen Sensoren und Abgleich	x	Unbegrenzt	Optisch		x
Künstliche DNS				x	Künstliche DNS, Mikrocodes	Verschiedenste Formen (fordert schlecht zugängliche Stelle)	Beliebig	Beliebig	Auftragen der DNS auf Oberfläche	UV-Licht, Mikroskop, DNS-Analyse	x	Unbegrenzt	• Optisch • Physikalisch	x	x
Digitaldruck / Prepress-Druckmerkmale	Digitales Wasserzeichen	x			Feine Muster	Alle bedruckbaren Materialien	Keine Einschränkungen bei Verwendung eines Etiketts	Als Etikett auf Produkt oder Verpackung	• Druckmaschine • Als Etikett: Aufkleben, Anhängen etc.	Optisch durch den Menschen evtl. mit Hilfsmitteln (Lupe)		Unbegrenzt	Optisch		x
Siebdruck / Prägen		x			• Fühlbarer Schriftzug. • (Bei Siebdruck: zumeist stark deckender Farbauftrag, hohe Schichtdicke, „salzgezahnartige" Siebstruktur an den Rändern.)	• Papiererzeugnisse • Kunststoffe • Textilien • Metall • Glas	• Wie Trägermaterial • beliebig (außer bei Etiketten)	• Produkt • Verpackung • Etikett	Druck-/Prägemaschine	Optisch/manuell/haptisch durch den Menschen		Unbegrenzt	• Optisch • Haptisch	x	x
Hologramme (OVD)		x			Hologramm(folie)	• Folien • Etiketten	• Beliebig (als Etikett) • direkt auf Kunststoff	• Verpackung • Etikett	• Aufkleben • integriert in Spritzgussform	Optische Prüfung von bestimmten Merkmalen (benötigt werden Mikroskop, Beleuchtung etc.)	(x)	Unbegrenzt	Optisch		x
Sicherheitsstreifen/ -faden		x			Metallischer Faden	• Papier • Stoff	• Identisch mit Papier • beliebig (bei Etikett)	• In das Produkt integriert • Produkt/Verpackung	Aufbringen eines Etiketts	Bloßes Auge, Scanner	(x)	Unbegrenzt	Optisch		x
Clusterfolie		x			Folie mit Farbkippeffekt	Nicht notwendig	Beliebig	• Produkt • Verpackung	Aufkleben (bei metallischen Oberfläche auch direkt aufbringen)	• Optisch durch den Menschen • Auslesen mit Handlesegerät möglich	(x)	Unbegrenzt	Optisch		x
Intagliodruck	Stichtiefedruck	x			Druckbild aus dickflüssiger, hochpigmentierter Farbe	Papier	Beliebig (bei Etikett)	• Verpackung • Etikett	Aufkleben eines Etiketts	Optisch/haptisch durch den Menschen		Unbegrenzt	• Optisch • Haptisch	x	x
Echtfarbenelemente			x		Farbpigmente außerhalb der üblichen rgb/cmyk-Werte	• Keines • bedruckbare Materialien als Etikett	• Alle bedruckbaren Materialien • beliebig (bei Etikett)	• Verpackung • Etikett • Oberfläche	Drucker	Optisch durch den Menschen		Unbegrenzt	Optisch		x
Kippfarbe	Optisch variable farben	x			Pigmente mit Farbkippeffekt	• Keines • Papier • Etikett	Beliebig	• Verpackung • Etikett	Drucker	Optisch durch den Menschen oder per Handscanner	(x)	Unbegrenzt	Optisch		x
Thermoreaktive, thermochrome, thermische Farbe		x			Thermoreaktive Farbpigmente evtl. auf Etikett	Bedruckbare Materialien	• Wie Trägermaterial • beliebig (bei Etikett)	• Verpackung • Etikett • Produkt	• Drucken • Aufkleben • etc.	Optisch durch den Menschen bei Temperaturveränderung		Einige Tausend Male	Thermisch (physikalisch & chemisch)	x	x
Fotochrome Farbe		x			Anorganische und organische photochrome Farbpigmente	Alle bedruckbaren Materialien	• Wie Trägermaterial • beliebig (bei Etikett)	• Verpackung • Etikett • Dokumente	Drucker	Optisch durch den Menschen		Mehrmals	Optisch		x
Farbcodes	Mikrofarbcodes		x		5-45 µm kleine Partikel aus Melamin-Alkyd-Polymer	• Evtl. Bindemittel • Feststoffe • Flüssigkeiten • Pasten • Pulver • Farben	Beliebig	• Integriert in Produkt • Oberflächenauftrag • Etikett • etc.	Abhängig vom Trägermaterial	Auflichtmikroskop oder „MicroReader" (Video-Mikroskop in Verbindung mit Notebook oder PC)	x	Unbegrenzt	Optisch		x
IR- /UV-Farbpigmente	Infrarotfarben		x		Farbpigmente (evtl. mit Trägermaterial)	• Folie • Etikett • Bindemittel/Lack • keines • etc.	Beliebig	• Verpackung • Etikett • Banknote	• Aufkleben • Drucken • etc.	Manuelle/elektronische IR-/UV-Prüfgeräte	x	Unbegrenzt	Optisch		x
Elektromagnetische Merkmale				x	Micro-Sicherheitsfaden	Als Gießharz auf allen Trägermaterialien möglich	Beliebig	• Verpackung • Etikett • Integration im Produkt	Oberflächenauftrag durch Hersteller, Anwender: Vermengen mit Grundmaterial des Produktes (z.B. Kunststoff, etc.)	Mobile Scanner	x	Unbegrenzt (entwerbar)	Elektro-magnetisch		x
Röntgenfluoreszenz			x		Markierungselemente, die normalerweise nicht Bestandteil des Produkts sind (z. B. Lanthanoide, Yttrium, Zink, Molybdän)	N/A	Beliebig	In das Produkt integriert	Während der Herstellung eingebracht	Röntgenfluoreszenzspektrograph	x	Unbegrenzt	• Elektro-magnetisch • Physikalisch		x
Sicherheitsanstanzung			x		Markierung am Verpackungskarton	Nicht notwendig	• Papier • Pappe • Kartonagen • Kunststoff • etc.	Teil der Verpackung	Integriert im Werkzeug (Produktionsprozess)	Optisch durch den Menschen		Unbegrenzt	Optisch		x

Detailliste technischer Schutzmaßnahmen ff.

Tabelle 2ff: Detailliste technischer Schutzmaßnahmen (erstellt von dem Verfasser in Anlehnung an Günthner, et al. 2010).

Sicherheit			Arten/ Ausprägungen	Typisches Einsatzgebiet	Speicherung von Daten			Erkennungswert beim Kunden			Anmerkungen
Kopiersicherheit	Manipulationssicherheit	Robustheit			Speichermöglichkeit/-art	Speichergröße	Beschreibbarkeit	Offen	Verborgen	Kommunikationsaufwand	
Hoch	Mechanisch zerstörbar, Übertragung muss durch geeignete Applikation verhindert werden.	Abhängig von der Applikation	• Banknoten • Dokumente	CDP, BitSecure, Speicherung von zusätzlichen Daten im Rauschmuster möglich	x Binäre Daten	In Abhängigkeit von der Größe des Musters (z.B. 96 bit)	Einmalig bei der Erzeugung des Musters	x		Offenes Merkmal, spezielle Prüfgeräte notwendig	N/A
Identische Kopien einfach möglich	Abhängig von Art der Kennzeichnung/Applikation	Abhängig von Art der Kennzeichnung/Applikation	• Logistik • Medizintechnik • etc.	Verschiedene Codes möglich (DataMatrix etc.)	x Ziffern, ASCII-Zeichen (abh. vom konkreten Code)	Abhängig vom konkreten Code und der Größe	Einmalig		x	Offenes Merkmal, welches dem Verbraucher bekannt ist. Prüfmittel und Infrastruktur (Datenverbindung) notwendig.	N/A
Sehr sicher (Schwankungen beim Druckprozess nicht reproduzierbar)	Merkmal kann zerstört werden, Übertragung muss durch geeignete Applikation verhindert werden	Abhängig von der konkreten Ausführung	Markierung von Verpackungen	Speicherung der Referenzdaten in zentraler Datenbank oder in 2D-Barcode, Speicherung von Zusatzdaten im Master möglich	Keine	N/A	N/A		x	Offenes Merkmal, spezielle Prüfgeräte oder zumindest Software notwendig, evtl. Datenverbindung notwendig	N/A
• Erzeugung neuer Transponder schwierig • 1:1-Kopie bei Systemen ohne Datenverschlüsselung möglich	Ablösen des Transponders kann je nach Befestigung einfach möglich sein. Zerstörung des Transponders prinzipiell durch mechanische Einflüsse möglich.	Einfluss von leitfähigen Materialien (Metall, Flüssigkeiten), Transponder-Inlay muss geschützt werden.	• Logistik • Werkzeugerkennung • Schließsysteme • etc.	Verschiedene Systeme (z.B. Frequenzen, Standards etc.)	x Digitale Daten auf Mikrochip	Bis mehrere hundert kByte	Einmalig oder wieder-beschreibbar	x	x	Informationen sind nur mit speziellen Lesegeräten auslesbar.	N/A
Nicht kopierbar	Bei bekannter Prüfstelle kann die Oberfläche mechanisch verändert werden.	Abhängig vom Werkstoff	• Verpackungen • Papier-, Metall-, Kunststoffoberflächen	Laseroberflächen-authentifizierung (Bayer ProtekXion) etc.	(x) Nur über verknüpfte Daten.	N/A	N/A		x	Verborgenes Merkmal.	N/A
Je nach Ausführung sehr hoch. Reproduzierung der DNS aufwendig.	Kann ohne großen Aufwand abgewischt werden sofern bekannt wo angebracht.	Muss vor Umwelteinflüssen geschützt werden.	Markierung von Gegenständen	Künstliche DNS, Mikrocodes, Microdust, "DNS-Dusche"	x DNS, Text	N/A	Einmalig		x		
Je nach Ausführung sehr hoch. Kann nicht mit Kopierern oder Scannern dupliziert werden, benötigt Spezialwissen und -ausstattung.	Zerstörung möglich. Übertragung nach Ablösen des Etiketts in Abhängigkeit von der Befestigungsart evtl. möglich.	Nicht für raue Umgebungsbedingungen geeignet.	• Ausweise • Banknoten • Dokumente	Guillochendruck, Mikrotext, digital erzeugte Wasserzeichen. Kombination mit UV-Farbe möglich.	(x) Keine, außer bei Mikrotext	N/A	N/A		x	Offenes Merkmal. Relativ einfach zu kommunizieren. Dennoch genaue Prüfung notwendig, um Kopien zu erkennen.	N/A
Drucktechnik im freien Handel verfügbar	Zerstörung möglich, Übertragung auf andere Produkte nicht möglich.	Robust gegenüber mechanischen und chemischen Beanspruchungen.	Folienaufdruck	N/A	x Schrift, Muster	N/A	Einmalig		x	Offenes Merkmal, Unterscheidung zu anderen Drucktechniken muss kommuniziert werden.	N/A
Komplexe Merkmale in Hologrammen sind nicht reproduzierbar. Wesentlich ist immer die genaue Prüfung.	Mechanisch zerstörbar, abhängig von Art der Applikation	Widerstandsfähig, limitierte UV-Stabilität	• Medizinprodukte • Verpackungen • Geldscheine	2D- und 3D-Hologramme	(x) In der Regel keine (bei Tesa Holospot: Einbringen einer Nummer möglich)	N/A (Sonderlösungen: bis 1024 Bit)	N/A (Sonder-lösungen: einmalig)	x		Offenes Merkmal. Nur einfache Merkmale können vom Endkunden geprüft werden. Jedes Prüfmerkmal muss dokumentiert und kommuniziert werden.	N/A
Sehr schwer kopierbar	Abhängig von Befestigung des Etiketts	Entfernung geht mit Beschädigung des Papiers einher.	• Banknoten • Dokumente	Cleartext, ColourShift, Country Code, eingebettet, Fenster, Hologramm	Keine	N/A	N/A	x		Offenes bekanntes Merkmal, im Gegenlicht gut erkennbar	N/A
Sehr hoch	Bei geeigneter Applikation sehr sicher. Zerstörung mechanisch möglich.	N/A	Verpackungen	Nano-Flakes, Nano-Cluster, ClusterSecure, i-Spec etc.	Keine	N/A	N/A	x		Offenes Merkmal. Relativ einfach zu kommunizieren	N/A
Sehr spezielle Drucktechnik notwendig	Abhängig von Applikation	N/A	• Banknoten • Pässe • Urkunden	N/A	x Text	N/A	N/A	x		Prüfen für Laien schwierig	N/A
Kann mit Standardkopierern nicht reproduziert werden.	Abhängig von der Ausführung (Untergrund etc.)	Ähnlich anderen Farben	• Eintrittskarten • Flugtickets • Fahrkarten	N/A	Keine	N/A	N/A	x		Offenes Merkmal. Einfach zu kommunizieren.	N/A
• teilweise frei käuflich • teilweise hochsicher	Ähnlich anderen Farben	Ähnlich anderen Farben	• Geldscheine • Verpackungen • Dokumente • Medikamente	Unterschiedliche Farbeffekte mit unterschiedlich hoher Sicherheit realisierbar	Keine	N/A	N/A	x		Offenes bekanntes Merkmal, genauer Farbumschlag muss kommuniziert werden.	N/A
Farben frei erhältlich	Abhängig von der Applikation	Gute kurzfristige Temperaturbeständigkeit bis 160°; geringe Lichtechtheit, Lackierung zum Schutz vor mechanischen Schäden und UV-Licht möglich.	• Produktetiketten • Verpackungen	Verschiedene Farben, verschiedene Farbumschläge bei unterschiedlichen Temperaturen	(x) Keine, Daten im Hintergrund möglich	N/A	N/A	x		Art der Prüfung muss kommuniziert werden	N/A
Kann nur mit speziellen fotochromer Farbe in richtiger Mischung kopiert werden.	Ähnlich wie andere Farben	Ähnlich wie andere Farben	N/A	N/A	Keine	N/A	N/A	x	x	Je nach Ausführung nicht offensichtlich. Merkmal muss kommuniziert werden.	N/A
Sehr hoch, da nur wenige Hersteller weltweit.	Partikel sind sehr widerstandsfähig und können kaum vollständig entfernt werden	Sehr widerstandsfähig	Vielfältig einsetzbar, vor allem: • Etiketten • Siegel • Spritzguss	Microcode, Microtaggant, Securag; Abwandlung: DataDotDNA	Keine	N/A	N/A		x	Kann nur mit Mikroskop erkannt werden.	DataDotDNA: Mit Seriennummern beschriftete Mikropunkte / Plättchen aus Polyestersubstrat.
IR-Farbe (Anti Stokes) und UV-Farbe teilweise frei zugänglich.	Evtl. mechanisch entfernbar	Abhängig vom Trägermaterial, sehr robust	• Banknoten • Medikamenten-verpackungen	IR-/UV-Farbe (verschiedene Wellenlängen)	Keine	N/A	N/A		x	Verdecktes Merkmal, einfache Prüfung	Sicherheitsniveau abhängig von Kombination und Codierung unterschiedlicher Pigmente
Legierung und spezielle physikalische Behandlung bei der Herstellung sind kaum rekonstruierbar.	Merkmale sind in großer Zahl auf-/einbringbar und daher nahezu nicht entfernbar. Übertragung muss über geeignete Applikation verhindert werden.	Robust	• Ersatzteile • Bekleidung • Dokumente • Chip- & Kreditkarten	MicroWire ®, DataTraceDNA®	Keine	N/A	N/A		x	Verdecktes Merkmal, spezielle Prüfgeräte notwendig, ohne Sichtkontakt prüfbar	N/A
Sehr hoch (Markierungselement muss erst erkannt werden)	N/A	Hoch	N/A	Nicht bekannt	Keine	N/A	N/A		x	Verdecktes Kennzeichen. Nur mit speziellen Geräten und Wissen erkennbar	N/A
• Merkmal ist kopierbar • Sicher ist das Merkmal nur solange es nicht bekannt wird	Das Merkmal kann mutwillig zerstört, jedoch nicht von einer Verpackung auf eine andere übertragen werden.	Merkmal ist so robust wie die markierte Verpackung.	Kartonverpackungen	Keine	Keine	N/A	N/A		x	Verborgenes Merkmal.	N/A

Foliensätze

Folgende Seiten sind dazu gedacht, die Ergebnisse dieser Arbeit möglichst einfach in eine Präsentation einbinden zu können. Die Foliensätze beinhalten jeweils zwei der in dieser Arbeit genannten technischen Schutzmaßnahmen, wobei versucht wurde, möglichst vergleichbare Maßnahmen auf eine Seite zu bekommen.

Die Foliensätze unterscheiden sich vom Rest der Arbeit insofern, als dass keine Quellenangaben für Inhalt und Bilder gemacht werden. Inhaltlich wiederholen sie die bereits in der Arbeit genannten Aussagen und beziehen sich auf die *Detailliste technischer Schutzmaßnahmen* in Anlehnung an Günthner, et al. (2010). Es wurde versucht die wichtigsten Merkmale aufzuführen, ohne eine unübersichtlich große Tabelle zu schaffen.
Die zusätzlich aufgeführten Bilder beziehen sich ausschließlich auf die Abbildungen nach Günthner, et al. (2010) oder auf bereits im obigen Text genannte Quellen und können in der besagten Originalquelle nachgeschlagen werden.

HOCHSCHULE FURTWANGEN UNIVERSITY HFU

Folien: Codes mit Rauschmuster // 2-D Barcode

Codes mit Rauschmuster	
Unikatskennzeichen	✓
Originalitätskennzeichen	
Offenes Merkmal	✓
Verborgenes Merkmal	
Speichermöglichkeit	✓
Kennzeichnung	Gedrucktes Rauschmuster
Ort der Kennzeichnung	• Produkt • Verpackung
Prüfungsmethode	Scanner, spezielles Lesegerät
Kopiersicherheit	Hoch
Manipulationssicherheit	Mechanisch zerstörbar, Übertragung muss durch geeignete Applikation verhindert werden
Robustheit	Abhängig von der Applikation

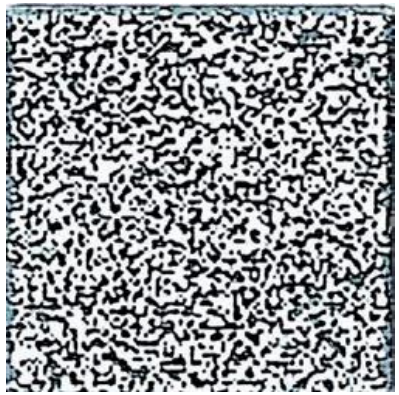

Abbildung: Copy Detection Pattern

Abbildung: 2-D Barcode.

2-D Barcode	
Unikatskennzeichen	✓
Originalitätskennzeichen	
Offenes Merkmal	✓
Verborgenes Merkmal	
Speichermöglichkeit	✓
Kennzeichnung	2-D Barcode
Ort der Kennzeichnung	Beliebig
Prüfungsmethode	2D-Barcode-Scanner
Kopiersicherheit	Identische Kopien einfach möglich
Manipulationssicherheit	Abhängig von Art der Kennzeichnung/Applikation
Robustheit	Abhängig von Art der Kennzeichnung/Applikation

HOCHSCHULE FURTWANGEN UNIVERSITY HFU

Folien: Stochastische Schwankungen im Druckbild // RFID

Stochastische Schwankungen im Druckbild	
Unikatskennzeichen	✓
Originalitätskennzeichen	
Offenes Merkmal	✓
Verborgenes Merkmal	
Speichermöglichkeit	✗
Kennzeichnung	Merkmal entsteht im Druckprozess
Ort der Kennzeichnung	• Produkt • Verpackung • Etikett
Prüfungsmethode	Spezielle Prüfgeräte, teilweise sind Handykameras etc. ausreichend.
Kopiersicherheit	Sehr sicher (Schwankungen beim Druckprozess nicht reproduzierbar)
Manipulationssicherheit	Merkmal kann zerstört werden, Übertragung muss durch geeignete Applikation verhindert werden
Robustheit	Abhängig von der konkreten Ausführung

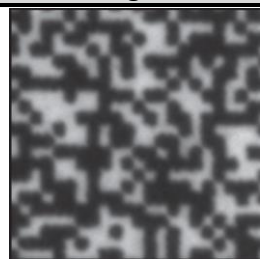

Abbildung: Stochastische Schwankungen im Druckbild

RFID	
Unikatskennzeichen	✓
Originalitätskennzeichen	
Offenes Merkmal	✓
Verborgenes Merkmal	✓
Speichermöglichkeit	✓
Kennzeichnung	IC mit Antenne zur (elektro)magnetischen Kopplung (Transponder)
Ort der Kennzeichnung	• Als Etikett auf Produkt oder Verpackung • integriert • etc.
Prüfungsmethode	Antenne, Lesegerät, Rechner/Steuerung
Kopiersicherheit	• Erzeugung neuer Transponder schwierig • 1:1-Kopie bei Systemen ohne Datenverschlüsselung möglich
Manipulationssicherheit	Ablösen des Transponders kann je nach Befestigung einfach möglich sein. Zerstörung des Transponders prinzipiell durch mechanische Einflüsse möglich.
Robustheit	Einfluss von leitfähigen Materialien (Metall, Flüssigkeiten), Transponder-Inlay muss geschützt werden.

HOCHSCHULE FURTWANGEN UNIVERSITY HFU

Folien: Oberflächenauthentifizierung // Künstliche DNA

Oberflächen-authentifizierung	
Unikatskennzeichen	✓
Originalitätskennzeichen	
Offenes Merkmal	
Verborgenes Merkmal	✓
Speichermöglichkeit	(✓)
Kennzeichnung	Oberflächenstruktur
Ort der Kennzeichnung	Definierte Stelle der (Bauteil-)Oberfläche
Prüfungsmethode	Mikroskopische Aufnahme mit optischen Sensoren und Abgleich
Kopiersicherheit	Nicht kopierbar
Manipulationssicherheit	Bei bekannter Prüfstelle kann die Oberfläche mechanisch verändert werden.
Robustheit	Abhängig vom Werkstoff

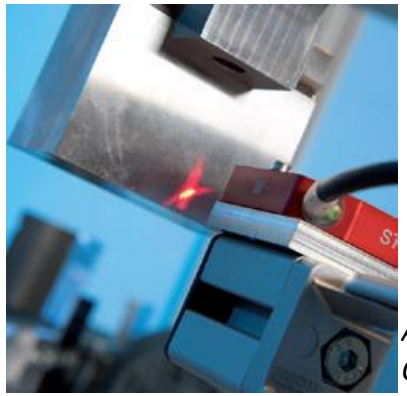

Abbildung: Oberflächenauthentifizierung

Künstliche DNS	
Unikatskennzeichen	✓
Originalitätskennzeichen	
Offenes Merkmal	
Verborgenes Merkmal	✓
Speichermöglichkeit	✓
Kennzeichnung	Künstliche DNS, Mikrocodes
Ort der Kennzeichnung	Beliebig
Prüfungsmethode	UV-Licht, Mikroskop, DNS-Analyse
Kopiersicherheit	Je nach Ausführung sehr hoch. Reproduzierung der DNS aufwendig.
Manipulationssicherheit	Kann ohne großen Aufwand abgewischt werden sofern bekannt wo angebracht.
Robustheit	Muss vor Umwelteinflüssen geschützt werden.

HOCHSCHULE FURTWANGEN UNIVERSITY HFU

Folien: Digitaldruck / Prepress-Druckmerkmale // Siebdruck / Prägen

Digitaldruck / Prepress-Druckmerkmale	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	✓
Verborgenes Merkmal	
Speichermöglichkeit	(✓)
Kennzeichnung	Feine Muster
Ort der Kennzeichnung	Als Etikett auf Produkt oder Verpackung
Prüfungsmethode	Optisch durch den Menschen evtl. mit Hilfsmitteln (Lupe)
Kopiersicherheit	Je nach Ausführung sehr hoch. Kann nicht mit Kopierern oder Scannern dupliziert werden, benötigt Spezialwissen und -ausstattung.
Manipulationssicherheit	Zerstörung möglich. Übertragung nach Ablösen des Etiketts in Abhängigkeit von der Befestigungsart evtl. möglich.
Robustheit	Nicht für raue Umgebungsbedingungen geeignet.

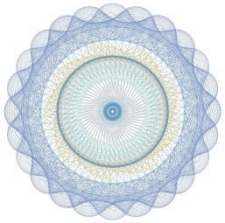

Abbildung: Guillochendruck.

Siebdruck / Prägen	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	✓
Verborgenes Merkmal	
Speichermöglichkeit	✓
Kennzeichnung	• Fühlbarer Schriftzug. • (Bei Siebdruck: zumeist stark deckender Farbauftrag, hohe Schichtdicke; „sägezahnartige“ Siebstruktur an den Rändern.)
Ort der Kennzeichnung	• Produkt • Verpackung • Etikett
Prüfungsmethode	Optisch/manuell/haptisch durch den Menschen
Kopiersicherheit	Drucktechnik im freien Handel verfügbar
Manipulationssicherheit	Zerstörung möglich, Übertragung auf andere Produkte nicht möglich.
Robustheit	Robust gegenüber mechanischen und chemischen Beanspruchungen.

HOCHSCHULE FURTWANGEN UNIVERSITY HFU

Folien: Hologramme (Optically Variable Device) // Sicherheitsstreifen /-faden

Hologramme (OVD)	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	✓
Verborgenes Merkmal	
Speichermöglichkeit	(✓)
Kennzeichnung	Hologramm(folie)
Ort der Kennzeichnung	• Verpackung • Etikett
Prüfungsmethode	Optische Prüfung von bestimmten Merkmalen (benötigt werden Mikroskop, Beleuchtung etc.)
Kopiersicherheit	Komplexe Merkmale in Hologrammen sind nicht reproduzierbar. Wesentlich ist immer die genaue Prüfung.
Manipulationssicherheit	Mechanisch zerstörbar, abhängig von Art der Applikation
Robustheit	Widerstandsfähig, limitierte UV-Stabilität

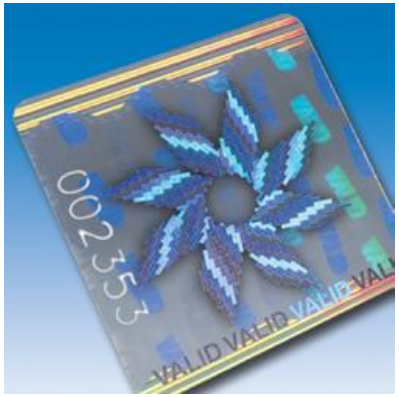

Abbildung: Hologramme.

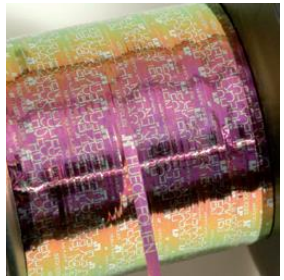

Abbildung: Sicherheitsfaden.

Sicherheitsstreifen/ -faden	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	✓
Verborgenes Merkmal	
Speichermöglichkeit	✗
Kennzeichnung	Metallischer Faden
Ort der Kennzeichnung	• In das Produkt integriert • Produkt/Verpackung
Prüfungsmethode	Bloßes Auge, Scanner
Kopiersicherheit	Sehr schwer kopierbar
Manipulationssicherheit	Abhängig von Befestigung des Etiketts
Robustheit	Entfernung geht mit Beschädigung des Papiers einher.

Folien: Clusterfolie // Intagliodruck (Stichtiefdruck)

Clusterfolie	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	✓
Verborgenes Merkmal	
Speichermöglichkeit	✗
Kennzeichnung	Folie mit Farbkippeffekt
Ort der Kennzeichnung	• Produkt • Verpackung
Prüfungsmethode	• Optisch durch den Menschen • Auslesen mit Handlesegerät möglich
Kopiersicherheit	Sehr hoch
Manipulationssicherheit	Bei geeigneter Applikation sehr sicher. Zerstörung mechanisch möglich.
Robustheit	N/A

Abbildung: Clusterfolie.

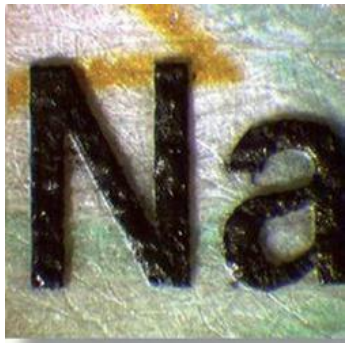

Abbildung: Intagliodruck.

Intagliodruck	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	✓
Verborgenes Merkmal	
Speichermöglichkeit	✓
Kennzeichnung	Druckbild aus dickflüssiger, hochpigmentierter Farbe
Ort der Kennzeichnung	• Verpackung • Etikett
Prüfungsmethode	Optisch/haptisch durch den Menschen
Kopiersicherheit	Sehr spezielle Drucktechnik notwendig
Manipulationssicherheit	Abhängig von Applikation
Robustheit	N/A

HOCHSCHULE FURTWANGEN UNIVERSITY HFU

Folien: Echtfarbenelemente // Kippfarbe (Optisch variable Farben)

Echtfarbenelemente	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	✓
Verborgenes Merkmal	
Speichermöglichkeit	✗
Kennzeichnung	Farbpigmente außerhalb der üblichen rgb/cmyk-Werte
Ort der Kennzeichnung	• Verpackung • Etikett • Oberfläche
Prüfungsmethode	Optisch durch den Menschen
Kopiersicherheit	Kann mit Standardkopierern nicht reproduziert werden.
Manipulationssicherheit	Abhängig von der Ausführung (Untergrund etc.)
Robustheit	Ähnlich anderen Farben

Abbildung: Echtfarbelemente.

Kippfarbe	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	✓
Verborgenes Merkmal	
Speichermöglichkeit	✗
Kennzeichnung	Pigmente mit Farbkippeffekt
Ort der Kennzeichnung	• Verpackung • Etikett
Prüfungsmethode	Optisch durch den Menschen oder per Handscanner
Kopiersicherheit	• teilweise frei käuflich • teilweise hochsicher
Manipulationssicherheit	Ähnlich anderen Farben
Robustheit	Ähnlich anderen Farben

Folien: Thermoreaktive, thermochrome, thermische Farbe // Fotochrome Farbe

Thermoreaktive, thermochrome, thermische Farbe	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	✓
Verborgenes Merkmal	
Speichermöglichkeit	(✓)
Kennzeichnung	Thermoreaktive Farbpigmente evtl. auf Etikett
Ort der Kennzeichnung	• Verpackung • Etikett • Produkt
Prüfungsmethode	Optisch durch den Menschen bei Temperaturveränderung
Kopiersicherheit	Farben frei erhältlich
Manipulationssicherheit	Abhängig von der Applikation
Robustheit	Gute kurzfristige Temperaturbeständigkeit bis 160°; geringe Lichtechtheit, Lackierung zum Schutz vor mechanischen Schäden und UV-Licht möglich.

Abbildung: Thermoreaktive Farbe.

Fotochrome Farbe	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	✓
Verborgenes Merkmal	✓
Speichermöglichkeit	✗
Kennzeichnung	Anorganische und organische photochrome Farbpigmente
Ort der Kennzeichnung	• Verpackung • Etikett • Dokumente
Prüfungsmethode	Optisch durch den Menschen
Kopiersicherheit	Kann nur mit spezieller fotochromer Farbe in richtiger Mischung kopiert werden.
Manipulationssicherheit	Ähnlich wie andere Farben
Robustheit	Ähnlich wie andere Farben

HOCHSCHULE FURTWANGEN UNIVERSITY HFU

Folien: Farbcodes (Mikrofarbcodes) // IR-/ UV-Farbpigmente (Infrarotfarben)

Farbcodes	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	
Verborgenes Merkmal	✓
Speichermöglichkeit	✗
Kennzeichnung	5-45 µm kleine Partikel aus Melamin-Alkyd-Polymer
Ort der Kennzeichnung	• Integriert in Produkt • Oberflächenauftrag • Etikett • etc.
Prüfungsmethode	Auflichtmikroskop oder „MicroReader“ (Video-Mikroskop in Verbindung mit Notebook oder PC)
Kopiersicherheit	Sehr hoch, da nur wenige Hersteller weltweit.
Manipulationssicherheit	Partikel sind sehr widerstandfähig und können kaum vollständig entfernt werden
Robustheit	Sehr widerstandsfähig

Abbildung: Farbcodes.

IR-/UV-Farbpigmente	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	
Verborgenes Merkmal	✓
Speichermöglichkeit	✗
Kennzeichnung	Farbpigmente (evtl. mit Trägermaterial)
Ort der Kennzeichnung	• Verpackung • Etikett • Banknote
Prüfungsmethode	Manuelle/ elektronische IR-/UV-Prüfgeräte
Kopiersicherheit	IR-Farbe (Anti Stokes) und UV-Farbe teilweise frei zugänglich.
Manipulationssicherheit	Evtl. mechanisch entfernbar
Robustheit	Abhängig vom Trägermaterial, sehr robust

HOCHSCHULE FURTWANGEN UNIVERSITY HFU

Folien: Elektromagnetische Merkmale // Röntgenfluoreszenz

Elektromagnetische Merkmale	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	
Verborgenes Merkmal	✓
Speichermöglichkeit	✗
Kennzeichnung	Micro-Sicherheitsfaden
Ort der Kennzeichnung	• Verpackung • Etikett • Integration im Produkt
Prüfungsmethode	Mobile Scanner
Kopiersicherheit	Legierung und spezielle physikalische Behandlung bei der Herstellung sind kaum rekonstruierbar.
Manipulationssicherheit	Merkmale sind in großer Zahl auf-/einbringbar und daher nahezu nicht entfernbar. Übertragung muss über geeignete Applikation verhindert werden.
Robustheit	Robust

Abbildung: Elektromagnetische Merkmale.

Röntgenfluoreszenz	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	
Verborgenes Merkmal	✓
Speichermöglichkeit	✗
Kennzeichnung	Markierungselemente, die normalerweise nicht Bestandteil des Produkts sind (z. B. Lanthanoide, Yttrium, Zink, Molybdän)
Ort der Kennzeichnung	In das Produkt integriert
Prüfungsmethode	Röntgenfluoreszenzspektrograph
Kopiersicherheit	Sehr hoch (Markierungselement muss erst erkannt werden)
Manipulationssicherheit	N/A
Robustheit	Hoch

Folien: Sicherheitsanstanzung

Sicherheitsanstanzung	
Unikatskennzeichen	
Originalitätskennzeichen	✓
Offenes Merkmal	
Verborgenes Merkmal	✓
Speichermöglichkeit	✗
Kennzeichnung	Markierung am Verpackungskarton
Ort der Kennzeichnung	Teil der Verpackung
Prüfungsmethode	Optisch durch den Menschen
Kopiersicherheit	• Merkmal ist kopierbar • Sicher ist das Merkmal nur solange es nicht bekannt wird
Manipulationssicherheit	Das Merkmal kann mutwillig zerstört, jedoch nicht von einer Verpackung auf eine andere übertragen werden.
Robustheit	Merkmal ist so robust wie die markierte Verpackung.

Abbildung: Sicherheitsanstanzung.