(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2004-532439
(P2004-532439A)
(43)公表日　平成16年10月21日(2004.10.21)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 12/14	G06F	12/14	560B	5B017
G06F 12/00	G06F	12/14	310K	5B082
G06F 15/00	G06F	12/14	320B	5B085
G09C 1/00	G06F	12/14	320E	5C076
G09C 5/00	G06F	12/14	520C	5J104

審査請求 未請求　予備審査請求 有　（全 155 頁）　最終頁に続く

(21)出願番号　特願2002-560325(P2002-560325)
(86)(22)出願日　平成14年1月25日(2002.1.25)
(85)翻訳文提出日　平成15年7月22日(2003.7.22)
(86)国際出願番号　PCT/US2002/002322
(87)国際公開番号　WO2002/060110
(87)国際公開日　平成14年8月1日(2002.8.1)
(31)優先権主張番号　60/264,333
(32)優先日　平成13年1月25日(2001.1.25)
(33)優先権主張国　米国(US)
(31)優先権主張番号　60/267,875
(32)優先日　平成13年2月8日(2001.2.8)
(33)優先権主張国　米国(US)
(31)優先権主張番号　60/267,899
(32)優先日　平成13年2月9日(2001.2.9)
(33)優先権主張国　米国(US)

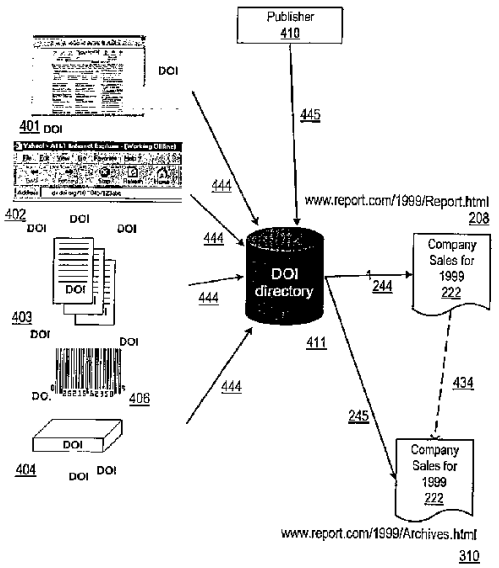
(71)出願人　503261971
デービッド・シドマン
アメリカ合衆国ニューヨーク州ブルックリン、９番ストリート５５８
(74)代理人　100110412
弁理士　藤元　亮輔
(72)発明者　デービッド・シドマン
アメリカ合衆国ニューヨーク州ブルックリン、９番ストリート５５８

Fターム(参考)　5B017 AA03 AA06 BA06 BA07 CA16
5B082 EA01 EA11 GA11
5B085 AA08 AE09 AE23 BG04 BG07
5C076 AA14 BA06
5J104 PA14

最終頁に続く

(54)【発明の名称】デジタル権利管理情報にアクセスするための装置、方法及びシステム

(57)【要約】
デジタル権利管理（ＤＲＭ）とコンテンツ流通システムは、固有の著作物をレファレンスして、配給、アクセス管理及び使用の追跡とワークのレポートを可能にする必要がある。ここに開示する装置、方法及びシステムは、当該システム内でのトランザクションの対象となり、著作物のインスタンス化に伴い移動する著作物の固有な識別子としてのデジタル・オブジェクト識別子（ＤＯＩ）を用いたＤＲＭ及びコンテンツ流通システムである。コンピュータからデジタル・ワークにアクセスする一つの方法を開示する。当該方法は、デジタル・ワークに少なくとも一つの使用権を関連付け、保護されたデジタル・ワークを作る。使用権はデジタル・ワークの表示、デジタル・ワークの複製、デジタル・ワークの別のコンピュータへの転送またはデジタル・ワークの印刷を含む。当該方法はデジタル・ワークに対しＤＯＩのような固有の識別子を選択し、保護されたデジタル・ワークと固有の識別子をデジタル著作物のライブラリやピア・ツー・ピア・ネットワークの一部のようなディレクトリに保存する。当該方法はコンピュータからディレクトリにクエリ



【特許請求の範囲】
【請求項１】
デジタル・ワークのための固有で永続的なユニバーサル・ネーム識別子を一つ選択することと、
少なくとも一つの使用権を該デジタル・ワークに関連付けて、保護されたデジタル・ワークを作ることと、
該保護されたデジタル・ワークと該固有で永続的なユニバーサル・ネーム識別子を、ユニバーサル・リソース・ネームと該ユニバーサル・リソース・ネームに関連する情報のための場所を維持するディレクトリに保存することと、
コンピュータから該ディレクトリにクエリーを発行し、該固有で永続的なユニバーサル・ネーム識別子を含む結果を一セット生成することと、
該ディレクトリから該固有で永続的なユニバーサル・ネーム識別子を持つ該保護されたデジタル・ワークを入手することと、
から成るコンピュータからデジタル・ワークにアクセスする方法。
【請求項２】
該固有で永続的なユニバーサル・ネーム識別子がデジタル・オブジェクト識別子（ＤＯＩ）であることを特徴とする請求項第１項に記載の方法。
【請求項３】
前記少なくとも一つの使用権によりユーザーが該コンピュータで該デジタル・ワークにアクションを行うことが可能になることを特徴とする請求項第１項に記載の方法。
【請求項４】
該アクションが該デジタル・ワークを表示することであることを特徴とする請求項第３項に記載の方法。
【請求項５】
該アクションが該デジタル・ワークを複製することであることを特徴とする請求項第３項に記載の方法。
【請求項６】
該アクションが該デジタル・ワークを別のコンピュータに転送することであることを特徴とする請求項第３項に記載の方法。
【請求項７】
該アクションが該デジタル・ワークを印刷することであることを特徴とする請求項第３項に記載の方法。
【請求項８】
該関連付けの後に、該保護されたデジタル・ワークを暗号化すること、
から更に成ることを特徴とする請求項第１項に記載の方法。
【請求項９】
該関連付けの後に、該保護されたデジタル・ワークを安全なコンテナにエンケースすることにより該保護されたデジタル・ワークをラッピングすること、
から更に成ることを特徴とする請求項第１項に記載の方法。
【請求項１０】
該安全なコンテナがデジタル・ウォーターマークを含むことを特徴とする請求項第９項に記載の方法。
【請求項１１】
該デジタル・ウォーターマークが該固有で永続的なユニバーサル・ネーム識別子を含むことを特徴とする請求項第１０項に記載の方法。
【請求項１２】
該保護されたデジタル・ワークと該固有で永続的なユニバーサル・ネーム識別子を説明するメタデータを保存すること、
から更に成る請求項第１項に記載の方法。
【請求項１３】

該クエリーが該メタデータを含むことを特徴とする請求項第１２項に記載の方法。
【請求項１４】
該コンピュータがモバイル・デバイスであることを特徴とする請求項第１項に記載の方法。
【請求項１５】
該ディレクトリがデジタル著作物をインデックスするカタログであることを特徴とする請求項第１項に記載の方法。
【請求項１６】
該ディレクトリがピア・ツー・ピア・ネットワークの一部であることを特徴とする請求項第１項に記載の方法。
【請求項１７】
コンテンツ配給業者、コンテテンツ・シンジゲーターあるいはコンテンツ集積業者が該コンピュータに代わって該クエリーを発行することを特徴とする請求項第１項に記載の方法。
【請求項１８】
固有で永続的なユニバーサル・ネーム識別子に関連するデジタル・ワークにアクセスする方法であって、別のコンピュータから保護されたデジタル・ワークを受信し、該保護されたデジタル・ワークが該デジタル・ワークと該デジタル・ワークに関連する少なくとも一つの使用権を含み、
ユニバーサル・リソース・ネームと該ユニバーサル・リソース・ネームに関連する情報のための場所を維持するディレクトリに該コンピュータからクエリーを発行し、該固有で永続的なユニバーサル・ネーム識別子を含む結果を一セット生成することと、
該保護されたデジタル・ワークの有効性を確認するために権利処理機関への接続を確立することと、
財務トランザクションの成功に応じて鍵を受信することと、
該鍵を使って、該保護されたデジタル・ワークに対する前記少なくとも一つの使用権により許可されたアクションを行うことにより該デジタル・ワークにアクセスすることと、
から成る該デジタル・ワークにアクセスする方法。
【請求項１９】
該固有で永続的なユニバーサル・ネーム識別子がデジタル・オブジェクト識別子（ＤＯＩ）であることを特徴とする請求項第１８項に記載の方法。
【請求項２０】
該権利処理機関がレポート・ログを更新することを特徴とする請求項第１８項に記載の方法。
【請求項２１】
該レポート・ログが売り上げデータを含むことを特徴とする請求項第２０項に記載の方法。
【請求項２２】
該レポート・ログが顧客データを含むことを特徴とする請求項第２０項に記載の方法。
【請求項２３】
該レポート・ログが電子的形式であり、該権利処理機関が定期的にレポート・ログを該デジタル・ワークの発行者に送ることを特徴とする請求項第２０項に記載の方法。
【請求項２４】
コンピュータからユニバーサル・リソース・ネームと該ユニバーサル・リソース・ネームに関連する情報のための場所を維持するディレクトリにクエリーを発行し、レファレンス・オプションのリストを得ることと、
該ディレクトリからクエリー結果を受信することと、
該クエリー結果に基づいてメニューを編成することと、
該メニューを表示して、該メニューを使用してユーザーが特定のレファレンス・オプションを選択しアクセスすることができるようにすることと、

から成る、一つの固有で永続的なユニバーサル・ネーム識別子に関連するデジタル・ワークにアクセスする方法。
【請求項２５】
該固有で永続的なユニバーサル・ネーム識別子を電子メールを介して送るメニュー・オプションを表示することから更に成る方法で、該電子メール送付のオプションを選択することが、該ユニバーサル・リソース・ネームが組み込まれた新規の電子メールをインスタンス化することを特徴とする請求項第２４項に記載の該方法。
【請求項２６】
デジタル・ワークのための固有で永続的なユニバーサル・ネーム識別子を一つ選択する手段と、
少なくとも一つの使用権を該デジタル・ワークに関連付ける手段で、保護されたデジタル・ワークを作る、該関連付ける手段と、
該保護されたデジタル・ワークと該固有で永続的なユニバーサル・ネーム識別子を、ユニバーサル・リソース・ネームと該ユニバーサル・リソース・ネームに関連する情報のための場所を維持するディレクトリに保存する手段と、
コンピュータから該ディレクトリにクエリーを発行する手段で、該固有で永続的なユニバーサル・ネーム識別子を含む結果を一セット生成する、該発行する手段と、
該ディレクトリから該固有で永続的なユニバーサル・ネーム識別子を持つ該保護されたデジタル・ワークを入手する手段と、
から成るコンピュータからデジタル・ワークにアクセスするためのシステム。
【請求項２７】
該固有で永続的なユニバーサル・ネーム識別子がデジタル・オブジェクト識別子（ＤＯＩ）であることを特徴とする請求項２６項に記載のシステム。
【請求項２８】
前記少なくとも一つの使用権によりユーザーが該コンピュータで該デジタル・ワークにアクションを行うことが可能になることを特徴とする請求項第２６項に記載のシステム。
【請求項２９】
該アクションが該デジタル・ワークを表示することであることを特徴とする請求項第２８項に記載のシステム。
【請求項３０】
該アクションが該デジタル・ワークを複製することであることを特徴とする請求項第２８項に記載のシステム。
【請求項３１】
該アクションが該デジタル・ワークを別のコンピュータに転送することであることを特徴とする請求項第２８項に記載のシステム。
【請求項３２】
該アクションが該デジタル・ワークを印刷することであることを特徴とする請求項第２８項に記載のシステム。
【請求項３３】
該関連付けの後に、該保護されたデジタル・ワークを暗号化する手段、
から更に成ることを特徴とする請求項第２６項に記載のシステム。
【請求項３４】
該関連付けの後に、該保護されたデジタル・ワークを安全なコンテナにエンケースすることにより該保護されたデジタル・ワークをラッピングする手段、
から更に成ることを特徴とする請求項第２６項に記載の方法。
【請求項３５】
該安全なコンテナがデジタル・ウォーターマークを含むことを特徴とする請求項第３４項に記載のシステム。
【請求項３６】
該デジタル・ウォーターマークが該固有で永続的なユニバーサル・ネーム識別子を含むこ

とを特徴とする請求項第３５項に記載のシステム。
【請求項３７】
該保護されたデジタル・ワークと該固有で永続的なユニバーサル・ネーム識別子を説明するメタデータを保存する手段と、
から更に成る請求項第２６項に記載のシステム。
【請求項３８】
該クエリーが該メタデータを含むことを特徴とする請求項第３７項に記載のシステム。
【請求項３９】
該コンピュータがモバイル・デバイスであることを特徴とする請求項第２６項に記載のシステム。
【請求項４０】
該ディレクトリがデジタル著作物をインデックスするカタログであることを特徴とする請求項第２６項に記載のシステム。
【請求項４１】
該ディレクトリがピア・ツー・ピア・ネットワークの一部であることを特徴とする請求項第２６項に記載のシステム。
【請求項４２】
コンテンツ配給業者、コンテテンツ・シンジゲーターあるいはコンテンツ集積業者が該コンピュータに代わって該クエリーを発行することを特徴とする請求項第２６項に記載のシステム。
【請求項４３】
固有で永続的なユニバーサル・ネーム識別子に関連するデジタル・ワークにアクセスするシステムであって、別のコンピュータから保護されたデジタル・ワークを受信し、該保護されたデジタル・ワークが該デジタル・ワークと該デジタル・ワークに関連する少なくとも一つの使用権を含み、
ユニバーサル・リソース・ネームと該ユニバーサル・リソース・ネームに関連する情報のための場所を維持するディレクトリに該コンピュータからクエリーを発行する手段で、該固有で永続的なユニバーサル・ネーム識別子を含む結果を一セット生成する、該発行する手段と、
該保護されたデジタル・ワークの有効性を確認するために権利処理機関への接続を確立する手段と、
財務トランザクションの成功に応じて鍵を受信する手段と、
該鍵を使って、該保護されたデジタル・ワークに対する前記少なくとも一つの使用権により許可されたアクションを行うことにより該デジタル・ワークにアクセスする手段と、
から成る該デジタル・ワークにアクセスするためのシステム。
【請求項４４】
該固有で永続的なユニバーサル・ネーム識別子がデジタル・オブジェクト識別子（ＤＯＩ）であることを特徴とする請求項第４３項に記載のシステム。
【請求項４５】
該権利処理機関がレポート・ログを更新することを特徴とする請求項第４３項に記載のシステム。
【請求項４６】
該レポート・ログが売り上げデータを含むことを特徴とする請求項第４５項に記載のシステム。
【請求項４７】
該レポート・ログが顧客データを含むことを特徴とする請求項第４５項に記載のシステム。
【請求項４８】
該レポート・ログが電子的形式であり、該権利処理機関が定期的にレポート・ログを該デジタル・ワークの発行者に送ることを特徴とする請求項第４５項に記載のシステム。

【請求項４９】
コンピュータからユニバーサル・リソース・ネームと該ユニバーサル・リソース・ネームに関連する情報のための場所を維持するディレクトリにクエリーを発行する手段で、レファレンス・オプションのリストを得る、該発行する手段と、
該ディレクトリからクエリー結果を受信する手段と、
該クエリー結果に基づいてメニューを編成する手段と、
該メニューを表示して、該メニューを使用してユーザーが特定のレファレンス・オプションを選択しアクセスすることができるようにする手段と、
から成る、一つの固有で永続的なユニバーサル・ネーム識別子に関連するデジタル・ワークにアクセスするためのシステム。
【請求項５０】
該固有で永続的なユニバーサル・ネーム識別子を電子メールを介して送るメニュー・オプションを表示することから更に成るシステムで、該電子メール送付のオプションを選択することが、該ユニバーサル・リソース・ネームが組み込まれた新規の電子メールをインスタンス化することを特徴とする請求項第４９項に記載の該システム。
【請求項５１】
プロセッサによって読み出し可能な媒体に保存されたプログラムで、
デジタル・ワークのための固有で永続的なユニバーサル・ネーム識別子を一つ選択するモジュールと、
少なくとも一つの使用権を該デジタル・ワークに関連付けるモジュールで、保護されたデジタル・ワークを作る、該関連付けるモジュールと、
該保護されたデジタル・ワークと該固有で永続的なユニバーサル・ネーム識別子を、ユニバーサル・リソース・ネームと該ユニバーサル・リソース・ネームに関連する情報のための場所を維持するディレクトリに保存するモジュールと、
コンピュータから該ディレクトリにクエリーを発行するモジュールで、該固有で永続的なユニバーサル・ネーム識別子を含む結果を一セット生成する、該発行するモジュールと、
該ディレクトリから該固有で永続的なユニバーサル・ネーム識別子を持つ該保護されたデジタル・ワークを入手するモジュールと、
から成る該プログラム。
【請求項５２】
該固有で永続的なユニバーサル・ネーム識別子がデジタル・オブジェクト識別子（ＤＯＩ）であることを特徴とする請求項５１項に記載の媒体。
【請求項５３】
前記少なくとも一つの使用権によりユーザーが該コンピュータで該デジタル・ワークにアクションを行うことが可能になることを特徴とする請求項第５１項に記載の媒体。
【請求項５４】
該アクションが該デジタル・ワークを表示することであることを特徴とする請求項第５３項に記載の媒体。
【請求項５５】
該アクションが該デジタル・ワークを複製することであることを特徴とする請求項第５３項に記載の媒体。
【請求項５６】
該アクションが該デジタル・ワークを別のコンピュータに転送することであることを特徴とする請求項第５３項に記載の媒体。
【請求項５７】
該アクションが該デジタル・ワークを印刷することであることを特徴とする請求項第５３項に記載の媒体。
【請求項５８】
該媒体が
該関連付けの後に、該保護されたデジタル・ワークを暗号化するモジュール、

から更に成ることを特徴とする請求項第５１項に記載の該媒体。
【請求項５９】
該媒体が
該関連付けの後に、該保護されたデジタル・ワークを安全なコンテナにエンケースすることにより該保護されたデジタル・ワークをラッピングするモジュール、
から更に成ることを特徴とする請求項第５１項に記載の該媒体。
【請求項６０】
該安全なコンテナがデジタル・ウォーターマークを含むことを特徴とする請求項第５９項に記載の媒体。
【請求項６１】
該デジタル・ウォーターマークが該固有で永続的なユニバーサル・ネーム識別子を含むことを特徴とする請求項第６０項に記載の媒体。
【請求項６２】
該保護されたデジタル・ワークと該固有で永続的なユニバーサル・ネーム識別子を説明するメタデータを保存するモジュールと、
から更に成る請求項５１項に記載の媒体。
【請求項６３】
該クエリーが該メタデータを含むことを特徴とする請求項第６２項に記載の媒体。
【請求項６４】
該コンピュータがモバイル・デバイスであることを特徴とする請求項第５１項に記載の媒体。
【請求項６５】
該ディレクトリがデジタル著作物をインデックスするカタログであることを特徴とする請求項第５１項に記載の媒体。
【請求項６６】
該ディレクトリがピア・ツー・ピア・ネットワークの一部であることを特徴とする請求項第５１項に記載の媒体。
【請求項６７】
コンテンツ配給業者、コンテテンツ・シンジゲーターあるいはコンテンツ集積業者が該コンピュータに代わって該クエリーを発行することを特徴とする請求項第５１項に記載の媒体。
【請求項６８】
プロセッサによって読み出し可能な媒体に保存されたプログラムで、固有で永続的なユニバーサル・ネーム識別子に関連するデジタル・ワークにアクセスする該プログラムであって、別のコンピュータから保護されたデジタル・ワークを受信し、該保護されたデジタル・ワークが該デジタル・ワークと該デジタル・ワークに関連する少なくとも一つの使用権を含み、該プログラムが、
ユニバーサル・リソース・ネームと該ユニバーサル・リソース・ネームに関連する情報のための場所を維持するディレクトリに該コンピュータからクエリーを発行するモジュールで、該固有で永続的なユニバーサル・ネーム識別子を含む結果を一セット生成する、該発行するモジュールと、
該保護されたデジタル・ワークの有効性を確認するために権利処理機関への接続を確立するモジュールと、
財務トランザクションの成功に応じて鍵を受信するモジュールと、
該鍵を使って、該保護されたデジタル・ワークに対する前記少なくとも一つの使用権により許可されたアクションを行うことにより該デジタル・ワークにアクセスするモジュールと、
から成る該プログラム。
【請求項６９】
該固有で永続的なユニバーサル・ネーム識別子がデジタル・オブジェクト識別子（ＤＯＩ

）であることを特徴とする請求項第６８項に記載の媒体。
【請求項７０】
該権利処理機関がレポート・ログを更新することを特徴とする請求項第６８項に記載の媒体。
【請求項７１】
該レポート・ログが売り上げデータを含むことを特徴とする請求項第７０項に記載の媒体。
【請求項７２】
該レポート・ログが顧客データを含むことを特徴とする請求項第７０項に記載の媒体。
【請求項７３】
該レポート・ログが電子的形式であり、該権利処理機関が定期的にレポート・ログを該デジタル・ワークの発行者に送ることを特徴とする請求項第７０項に記載の媒体。
【請求項７４】
一つの固有で永続的なユニバーサル・ネーム識別子に関連するデジタル・ワークにアクセスするための、プロセッサによって読み出し可能な媒体に保存されたプログラムで、
コンピュータからユニバーサル・リソース・ネームと該ユニバーサル・リソース・ネームに関連する情報のための場所を維持するディレクトリにクエリーを発行するモジュールで、レファレンス・オプションのリストを得る、該発行するモジュールと、
該ディレクトリからクエリー結果を受信するモジュールと、
該クエリー結果に基づいてメニューを編成するモジュールと、
該メニューを表示して、該メニューを使用してユーザーが特定のレファレンス・オプションを選択しアクセスすることができるようにするモジュールと、
から成る該プログラム。
【請求項７５】
該固有で永続的なユニバーサル・ネーム識別子を電子メールを介して送るメニュー・オプションを表示することから更に成る媒体で、該電子メール送付のオプションを選択することが、該ユニバーサル・リソース・ネームが組み込まれた新規の電子メールをインスタンス化することを特徴とする請求項第７４項に記載の該媒体。
【請求項７６】
プロセッサと、
該プロセッサに通信するよう接続されたメモリと、
該メモリに保存されたプログラムで、
デジタル・ワークのための固有で永続的なユニバーサル・ネーム識別子を一つ選択するモジュールと、
少なくとも一つの使用権を該デジタル・ワークに関連付けるモジュールで、保護されたデジタル・ワークを作る、該関連付けるモジュールと、
該保護されたデジタル・ワークと該固有で永続的なユニバーサル・ネーム識別子を、ユニバーサル・リソース・ネームと該ユニバーサル・リソース・ネームに関連する情報のための場所を維持するディレクトリに保存するモジュールと、
コンピュータから該ディレクトリにクエリーを発行するモジュールで、該固有で永続的なユニバーサル・ネーム識別子を含む結果を一セット生成する、該発行するモジュールと、
該ディレクトリから該固有で永続的なユニバーサル・ネーム識別子を持つ該保護されたデジタル・ワークを入手するモジュールと、
を含む、該プログラムと、
から成る、装置。
【請求項７７】
該固有で永続的なユニバーサル・ネーム識別子がデジタル・オブジェクト識別子（ＤＯＩ）であることを特徴とする請求項７６項に記載の装置。
【請求項７８】
前記少なくとも一つの使用権によりユーザーが該コンピュータで該デジタル・ワークにア

クションを行うことが可能になることを特徴とする請求項第７６項に記載の装置。
【請求項７９】
該アクションが該デジタル・ワークを表示することであることを特徴とする請求項第７８項に記載の装置。
【請求項８０】
該アクションが該デジタル・ワークを複製することであることを特徴とする請求項第７８項に記載の装置。
【請求項８１】
該アクションが該デジタル・ワークを別のコンピュータに転送することであることを特徴とする請求項第７８項に記載の装置。
【請求項８２】
該アクションが該デジタル・ワークを印刷することであることを特徴とする請求項第７８項に記載の装置。
【請求項８３】
該装置が
該関連付けの後に、該保護されたデジタル・ワークを暗号化するモジュール、
から更に成ることを特徴とする請求項第７６項に記載の該装置。
【請求項８４】
該装置が
該関連付けの後に、該保護されたデジタル・ワークを安全なコンテナにエンケースすることにより該保護されたデジタル・ワークをラッピングするモジュール、
から更に成ることを特徴とする請求項第７６項に記載の該装置。
【請求項８５】
該安全なコンテナがデジタル・ウォーターマークを含むことを特徴とする請求項第８４項に記載の装置。
【請求項８６】
該デジタル・ウォーターマークが該固有で永続的なユニバーサル・ネーム識別子を含むことを特徴とする請求項第８５項に記載の装置。
【請求項８７】
該保護されたデジタル・ワークと該固有で永続的なユニバーサル・ネーム識別子を説明するメタデータを保存するモジュールと、
から更に成る請求項７６項に記載の装置。
【請求項８８】
該クエリーが該メタデータを含むことを特徴とする請求項第８７項に記載の装置。
【請求項８９】
該コンピュータがモバイル・デバイスであることを特徴とする請求項第７６項に記載の装置。
【請求項９０】
該ディレクトリがデジタル著作物をインデックスするカタログであることを特徴とする請求項第７６項に記載の装置。
【請求項９１】
該ディレクトリがピア・ツー・ピア・ネットワークの一部であることを特徴とする請求項第７６項に記載の装置。
【請求項９２】
コンテンツ配給業者、コンテテンツ・シンジゲーターあるいはコンテンツ集積業者が該コンピュータに代わって該クエリーを発行することを特徴とする請求項第７６項に記載の装置。
【請求項９３】
プロセッサと、
該プロセッサに通信するよう接続されたメモリと、

該メモリに保存されたプログラムで、固有で永続的なユニバーサル・ネーム識別子に関連するデジタル・ワークにアクセスする該プログラムであって、別のコンピュータから保護されたデジタル・ワークを受信し、該保護されたデジタル・ワークが該デジタル・ワークと該デジタル・ワークに関連する少なくとも一つの使用権を含み、該プログラムが、
ユニバーサル・リソース・ネームと該ユニバーサル・リソース・ネームに関連する情報のための場所を維持するディレクトリに該コンピュータからクエリーを発行するモジュールで、該固有で永続的なユニバーサル・ネーム識別子を含む結果を一セット生成する、該発行するモジュールと、
該保護されたデジタル・ワークの有効性を確認するために権利処理機関への接続を確立するモジュールと、
財務トランザクションの成功に応じて鍵を受信するモジュールと、
該鍵を使って、該保護されたデジタル・ワークに対する前記少なくとも一つの使用権により許可されたアクションを行うことにより該デジタル・ワークにアクセスするモジュールと、
を含む、該プログラムと、
から成る、装置。

【請求項９４】

該固有で永続的なユニバーサル・ネーム識別子がデジタル・オブジェクト識別子（ＤＯＩ）であることを特徴とする請求項第９３項に記載の装置。

【請求項９５】

該権利処理機関がレポート・ログを更新することを特徴とする請求項第９３項に記載の装置。

【請求項９６】

該レポート・ログが売り上げデータを含むことを特徴とする請求項第９５項に記載の装置。

【請求項９７】

該レポート・ログが顧客データを含むことを特徴とする請求項第９５項に記載の媒体。

【請求項９８】

該レポート・ログが電子的形式であり、該権利処理機関が定期的にレポート・ログを該デジタル・ワークの発行者に送ることを特徴とする請求項第９５項に記載の媒体。

【請求項９９】

プロセッサと、
該プロセッサに通信するよう接続されたメモリと、
該メモリに保存されたプログラムで、固有で永続的なユニバーサル・ネーム識別子に関連するデジタル・ワークにアクセスする該プログラムであって、該プログラムが、
コンピュータからユニバーサル・リソース・ネームと該ユニバーサル・リソース・ネームに関連する情報のための場所を維持するディレクトリにクエリーを発行するモジュールで、レファレンス・オプションのリストを得る、該発行するモジュールと、
該ディレクトリからクエリー結果を受信するモジュールと、
該クエリー結果に基づいてメニューを編成するモジュールと、
該メニューを表示して、該メニューを使用してユーザーが特定のレファレンス・オプションを選択しアクセスすることができるようにするモジュールと、
を含む、該プログラムと、
から成る、装置。

【請求項１００】

該固有で永続的なユニバーサル・ネーム識別子を電子メールを介して送るメニュー・オプションを表示することから更に成る装置で、該電子メール送付のオプションを選択することが、該ユニバーサル・リソース・ネームが組み込まれた新規の電子メールをインスタンス化することを特徴とする請求項第９９項に記載の該装置。

【発明の詳細な説明】

【技術分野】
【０００１】
［関連出願］
本出願では以下の米国特許仮出願に対して、ここに優先権を主張する。（１）２００１年１月２５日に申請された、シリアル番号６０／２６４，３３３の「ＤＯＩとのレファレンス・リンキング」（弁護士ドケット番号４１８８－４００１）、（２）２００１年2月１４日に申請された、シリアル番号６０／２６８，７６６の「情報アクセスを実行する多重解決（マルチプル・レゾリューション）のための装置、方法及びシステム」（弁護士ドケット番号４１８８－４００２）、（３）２００１年3月１６日に申請された、シリアル番号６０／２７６，４５９の「情報アクセスを実行する登録のための装置、方法及びシステム」（弁護士ドケット番号４１８８－４００３）、（４）２００１年3月２９日に申請された、シリアル番号６０／２７９，７９２の「ディレクトリの品質保証のための装置、方法及びシステム」（弁護士ドケット番号４１８８－４００４）、（５）２００１年7月１０日に申請された、シリアル番号６０／３０３，７６８の「デジタル権利管理情報にアクセスするのための装置、方法及びシステム」（弁護士ドケット番号４１８８－４００５）、（６）２００１年１０月9日に申請された、シリアル番号６０／３２８，２７５の「デジタル権利管理情報にアクセスするのための装置、方法及びシステム」（弁護士ドケット番号４１８８－４００５ＵＳ１）、（７）２００１年2月８日に申請された、シリアル番号６０／２６７，８７５の「情報にアクセスするのための装置、方法及びシステム」（弁護士ドケット番号４１８８－４００６）、（８）２００１年2月9日に申請された、シリアル番号６０／２６７，８９９の「情報にアクセスするのための装置、方法及びシステムのための仮申請」（弁護士ドケット番号４１８８－４００７）、（９）２００１年2月２１日に申請された、シリアル番号６０／２７０，４７３の「ＤＯＩのためのビジネス・バリューと実施の考慮」（弁護士ドケット番号４１８８－４００８）、（１０）２００１年１０月9日に申請された、シリアル番号６０／３２８，２７４の「ピア環境において情報アクセスを実行するための装置、方法及びシステム」（弁護士ドケット番号４１８８－４０１０）、（１１）２００１年１０月9日に申請された、シリアル番号６０／３２８，２７０の「情報アクセスを追跡するための装置、方法及びシステム」（弁護士ドケット番号４１８８－４０１１）。これらの出願書はそれぞれ参照により開示に含まれる。
【０００２】
本出願書にはまた、以下の特許協力条約（ＰＣＴ）出願も参照により含まれる。（１２）デイビッド・シドマンの名義で２００２年1月２５日に申請された、「情報アクセスを実行する多重解決のための装置、方法及びシステム」（弁護士ドケット番号４１８８－４００２ＰＣ）、（１３）デイビッド・シドマンの名義で２００２年1月２５日に申請された、「情報アクセスを実行する登録のための装置、方法及びシステム」（弁護士ドケット番号４１８８－４００３ＰＣ１）、（１４）デイビッド・シドマンの名義で２００２年1月２５日に申請された、「ディレクトリ品質保証のための装置、方法及びシステム」（弁護士ドケット番号４１８８－４００４ＰＣ）、（１５）デイビッド・シドマンの名義で２００２年1月２５日に申請された、「ピア環境において情報アクセスを実行するための装置、方法及びシステム」（弁護士ドケット番号４１８８－４０１０ＰＣ）及び（１６）デイビッド・シドマンの名義で２００２年1月２５日に申請された、「情報アクセスを追跡するための装置、方法及びシステム」（弁護士ドケット番号４１８８－４０１１ＰＣ）。
【０００３】
ここに開示する発明は、デジタル権利管理システムによって保護されているデジタル著作物にアクセスするための装置、方法及びシステムである。より詳しくは、ここに開示する発明は、デジタル・オブジェクト識別子をデジタル権利管理システムに組み込み、システムをより耐久性があるものにし、多重解決、レポート、ウォーターマーキング、有効性確認の機能を提供する。
【背景技術】
【０００４】

［インターネット］
インターネットの利用が増えるにつれて、インターネット上で利用可能な情報の量も増加する。インターネット上に存在する情報は、コンピュータ・ソフトウェア、データベース、検討リスト、電子ジャーナル、ライブラリ・カタログ、オンライン情報サービス、メーリング・リスト、ニュース・グループ、ストリーミング・メディア等、数多くのフォーマットのドキュメントを含む様々な種類のものがある。幸いにもインターネット上のほとんどの情報には、ユーザーが利用しやすい方法でネットワークとインタラクションするためのウェブ・ブラウザを用いワールド・ワイド・ウェブを介してアクセスすることができる。

【０００５】
［ネットワーク］
一般にネットワークは、クライアント、サーバー及びグラフ・トポロジーにおける中間のノードの相互接続と相互運用から成ると考えられている。注意すべきことは、ここでは「サーバー」という用語は通常、通信ネットワーク全体の遠隔ユーザーのリクエストを処理したりそれに応答したりするためのコンピュータ、その他の機器、ソフトウェア、またはそれらの組み合わせを指すということである。サーバーはリクエストしてくる「クライアント」に情報を提供する。情報やリクエストを可能にしたり、処理、及び／またはソース・ユーザーからデスティネーション・ユーザーへの情報の流れを支援するコンピュータ、その他の機器、ソフトウェア、またはそれらの組み合わせは、通常「ノード」と呼ばれる。ネットワークは一般的にソース・ポイントからデスティネーションへの情報の転送を可能にするものと考えられている。
［伝送制御プロトコル／インターネット・プロトコル（ＴＣＰ／ＩＰ）］
コンピュータ・システム、データベース及びコンピュータ・ネットワークの拡散と拡大は、一般的にインターネットと称されるそのようなシステムの相互接続と国境を越えた通信ネットワークによって促進されてきた。インターネットは伝送制御プロトコルとインターネット・プロトコル（ＴＣＰ／ＩＰ）を発展させ、またその大部分においてそれらを用いている。ＴＣＰ／ＩＰは様々な変化するネットワーク業者によって形成された複数のネットワークを、ネットワークのネットワークのための基礎として相互接続するための、つまりインターネットのための米国国防総省（ＤｏＤ）の研究プロジェクトによって開発された。一つにはＤｏＤが、戦闘の最中に損害を受けても作動し続けることによって、通信ネットワークの損害を受けた部分を回避してデスティネーション・アドレスに情報を送るネットワークを必要としたことがＴＣＰ／ＩＰの開発の原動力となった。もちろん、ソース・アドレスのロケーションまたはデスティネーション・アドレスのロケーション自体が動作不能になった場合は、そのような伝達は不可能である。
インターネットはパケット交換型のネットワークであるため、インターネット上の情報はパケットと呼ばれる幾つもの断片に分割され、パケット形式で送信される。パケットはヘッダーと呼ばれるＩＰアドレス情報を含み、それらはルータがインターネット上の中間ノードを通してパケットをソースからデスティネーションへ配信することを可能にする。デスティネーションに到着すると、パケットは再構築されオリジナルのメッセージを形成し、欠落しているパケットがあれば、それらは再びリクエストされる。

【０００６】
プロトコルのＩＰ部分は、４バイトのアドレス・メカニズムに基づいて情報パケットをルーティングする役目を担う。アドレスはドットによって分離された４つの数字であり、各数字は０から２５５の範囲内で、例えば、「１２３．２５５．０．１２３」というようになる。ＩＰアドレスはインターネット当局及び登録機関が指定し、それぞれ固有のものである。

【０００７】
プロトコルのＴＣＰ部分は情報のパケットがソースからデスティネーションに正確に受信されたかを確認し、またもし正確に受信されなかった場合は、間違ったパケットを再送信するために用いられる。ユーザー・データグラム・プロトコル（ＵＤＰ）等の、配信を保

証しないその他の伝送制御プロトコルも一般的に利用されている。

［ワールド・ワイド・ウェブ］

インターネット、特にワールド・ワイド・ウェブ（ウェブ）が広く受け入れられ拡大し、膨大且つ多様な情報が集められた。情報技術システムを有するユーザー同士（つまりコンピュータ利用者）のインタラクションを可能にする様々なユーザー・インターフェースが現在利用されている。ＷｏｒｌｄＷｉｄｅＷｅｂ．ａｐｐ（ウェブ）と呼ばれる情報ナビゲーション・インターフェースは、１９９０年後半に開発された。その後、ウェブ・ブラウザ等の情報ナビゲーション・インターフェースがほぼ全てのコンピュータ・オペレーティング・システム・プラットフォームにおいて広く利用可能になった。

一般的にウェブは、複数のユーザー・インターフェース（例えばウェブ・ブラウザ）、サーバー、配信された情報、プロトコル及び仕様の、相乗相互運用の発現でありその結果である。ウェブ・ブラウザは情報へのナビゲーションとアクセスを促進するために設計され、一方情報サーバーは情報の供給を促進するために設計されている。通常ウェブ・ブラウザと情報サーバーは通信ネットワークを介してお互いに交信するように配置してある。情報サーバーは、通常ウェブ・ブラウザを用いて情報にアクセスするユーザーに対し情報を提供する機能を果たす。従って、情報サーバーは主にウェブ上の情報へのナビゲーションやアクセスにウェブ・ブラウザを用いるユーザーに対し情報を提供する。ウェブ・ブラウザの例としては、マイクロソフト社のインターネット・エクスプローラや、ネットスケープ・ナビゲーターがある。加えて、ウェブＴＶのようなナビゲーション・ユーザー・インターフェース機器もウェブ・ナビゲーションを容易にするために実現されている。マイクロソフト社のインフォメーション・サーバーやアパッチが情報サーバーの例として挙げられる。

［ユニバーサル・リソース・ロケーター（ＵＲＬ）］

ウェブの拡大は膨大な量の情報をもたらし、かかる膨大な情報はユニバーサル・リソース・ロケーター（ＵＲＬ）を利用することによりアクセス可能である。ＵＲＬとは通常ウェブ・ページ中にハイパーリンクとして組み入れられるアドレス、あるいはウェブ・ブラウザにタイプ入力されるアドレスである。所与のリソース（最も一般的には遠隔コンピュータ上にあるファイル）のＵＲＬはそのリソースのみを指す。一般的に、当該場所へのレファレンスは、例えば「ｈｔｔｐ：／／ｗｗｗ．ａＷｅｂＳｉｔｅ．ｃｏｍ／ａＦｏｌｄｅｒ／ａＦｉｌｅ／ａＦｉｌｅ．ｈｔｍｌ」というように、ディレクトリ・パス及びファイル名と併せて未解決のＩＰアドレスを用いて達成される。この例では、このＵＲＬが「ａＷｅｂＳｉｔｅ．ｃｏｍ」というドメインの「ｗｗｗ」という名前のコンピュータに接続し、そのコンピュータの「ａＦｏｌｄｅｒ」というディレクトリに保存されている「ａＦｉｌｅ．ｈｔｍｌ」という名前のファイルをリクエストするように、ブラウザに命じることになる。

［ユニバーサル・ネーム識別子（ＵＮＩ）］

Ｔｈｅ Ｃｏｒｐｏｒａｔｉｏｎ ｆｏｒ Ｎａｔｉｏｎａｌ Ｒｅｓｅａｒｃｈ Ｉｎｉｔｉａｔｉｖｅは、情報の名前と所在を指定するハンドル・システムと呼ばれる新しい手段を創り出し実施した。ハンドル・システムは現在のＵＲＬの利用状況を改善するために設計された。

ハンドル・システムは、インターネット上で情報の所在を確認したり情報を配信するための間接指定のレベルを導入する。ハンドル・システムは、リソースに名前を付けるための汎用システムである。特定のリソースの現在の場所に基づくＵＲＬを指定する代わりに、リソースにユニバーサル・ネーム識別子を指定する。ＵＮＩはユニバーサル・リソース識別子（ＵＲＩ）の一形式である。ＵＲＩはＵＮＩとＵＲＬの両方を含む。ＵＮＩはＵＲＬと違い、リソースの場所やその他の属性の変化に関わらず永続的なリソースの名前として機能し、またこれ以降そのような名前であるものとみなす。言い換えると、ユニバーサル・リソース・ネーム（ＵＲＮ）はＵＮＩの一種である（即ち、ＵＮＩはＵＲＮの概念を含む）。更に、ハンドルとはＵＲＮの一種である。またデジタル・オブジェクト識別子（ＤＯＩ）はハンドルの一種である。従って、ハンドル、ＵＲＮ、ＤＯＩ及び／またはその他

が様々な形式のＵＮＩに含まれる。ＵＮＩの様々な用語及び／または形式は、本文全体にわたって置換可能なように用いられ、特に明記しない限り置換可能と想定してよいものとする。ハンドルは、名付けられたリソースの現在のネットワーク上の場所及び当該の関連サービスの場所と共にハンドル・システムに登録される固有の名前である。この場所に関する情報は通常ＵＲＬの形式をとる。一般的なハンドルの種類の一つとしてデジタル・オブジェクト識別子（ＤＯＩ）が知られている。その場合ハンドルはＵＲＬの代わりにユーザーに配信され、表面上はハイパーリンクと同様に機能するかに見える。ユーザーがハンドルに遭遇すると、ユーザーのブラウザにハンドル・リクエストを行う作成する機能がある限りは、ユーザーはＵＲＬハイパーリンクを選択したり入力したりするのと同様にハンドルを選択したり入力したりする。そのような遭遇により、リソースの現在の場所を検索する自動のプロセスが始動する。リソースの現在の場所は、ハンドル・システムが提供するディレクトリの中のリソースのハンドルに関連付けられていて、ユーザーをリソースの現在の場所へと導く。同様のプロセスが作動し、ユーザーは識別されたワークに関連するサービスへとリダイレクトされる。ＵＲＬとは違い、リソースまたはサービスが移動した場合、ハンドル・システムのディレクトリのエントリーは更新可能なので、ハンドルと、ハンドルが特定するリソースまたはサービスとの永続的な関連付けが確保される。所与のリソースのＵＲＬのみを知っているということは、現実の世界において、ある人の住所だけ知っていて名前は知らないようなものである。もしその人が街の反対側へ引っ越した場合、名前を知らなければ探すのは非常に困難になる。ハンドル・システムにより、ハンドルを用いてリソースに永続的な名前を付けることができ、ハンドル・システム・ディレクトリの中のリソースの名前に基づいて、リソースの現在の場所を検索することができる。

［デジタル権利管理（ＤＲＭ）］

デジタル権利管理（ＤＲＭ）は、所有者の資産に対する所有権の説明、階層化、分析、評価、取引及びモニタリングに関係する。ＤＲＭは、ワークの物理的マニフェステーション（例えばテキストブック等）に対する所有権、あるいはワークのデジタル・マニフェステーション（例えばウェブ・ページ等）に対する所有権の管理を網羅する。ＤＲＭはまた、資産価値の有形・無形に関わらず、資産の管理を網羅する。現在のＤＲＭシステムは、資産の使用についての条件を説明するための文言、コントロールされた環境またはエンコードされた資産マニフェステーションを施行することにより資産の使用を追跡すること、及びデジタル権利の全体的管理のためのクローズド・アーキテクチャを含む。現在のＤＲＭシステムは一般に、ＵＲＬのような場所に基づく識別子に依存するため、場所に基づく識別子の柔軟性の無さによる制限を受けている。

【０００８】

そのため、ＤＲＭシステムに保護されたデジタル化された著作物に確実にアクセスするための装置、方法及びシステムが必要とされている。ここに開示する当該の装置、方法及びシステムはＤＲＭシステムの耐久性を改善し、ＤＲＭの顧客とコンテンツ発行者の両方に更なる能力を提供し、電子商取引の成長を促進するものである。

【発明の開示】

【課題を解決するための手段】

【０００９】

デジタル権利管理（ＤＲＭ）とコンテンツ流通システムは、配給、アクセス管理及び使用の追跡とワークのレポートを可能にするために、固有の著作物をレファレンスする必要がある。ここに開示する装置、方法及びシステムは、当該システム内でのトランザクションの対象となり、著作物のインスタンス化に伴い移動する著作物の固有な識別子としてのデジタル・オブジェクト識別子（ＤＯＩ）を用いたＤＲＭ及びコンテンツ流通システムである。

【００１０】

コンピュータからデジタル・ワークにアクセスする一つの方法を開示する。当該方法は、デジタル・ワークに少なくとも一つの使用権を関連付け、保護されたデジタル・ワークを作る。使用権はデジタル・ワークの表示、デジタル・ワークの複製、デジタル・ワークの

別のコンピュータへの転送またはデジタル・ワークの印刷を含む。当該方法はデジタル・ワークに対しＤＯＩのような固有の識別子を選択し、保護されたデジタル・ワークと固有の識別子をデジタル著作物のライブラリやピア・ツー・ピア・ネットワークの一部のようなディレクトリに保存する。当該方法はコンピュータからディレクトリにクエリーを発行し、固有の識別子を含む結果を一セット生成する。当該方法は固有の識別子を用い、保護されたデジタル・ワークをディレクトリから入手する。

【００１１】

別の実施例では、当該方法は保護されたデジタル・ワークを、従来技術の暗号化アルゴリズムを用いて暗号化するか、及び／または保護されたデジタル・ワークを安全なコンテナでラッピングする。安全なコンテナとは、従来技術のウォーターマーキング・アルゴリズムを用いたデジタル・ウォーターマークを含むこともできるし、デジタル・ワークに関連する固有の識別子を含むウォーターマーキング・アルゴリズムを用いることもできる。

別の実施例においては、当該方法は保護されたデジタル・ワークを説明するメタデータを保存し、メタデータをコンピュータからのクエリーに含む。更にまた、クエリーはユーザーに連結したコンピュータから生成されてもよいし、コンテンツ流通業者、コンテテンツ・シンジゲーターあるいはコンテンツ集積業者等の第三者からされてもよい。

【００１２】

添付した図面は、デジタル・オブジェクト識別子をデジタル権利管理システムに組み込むための装置、方法及びシステムの詳細を、その構造と動作の両方に関して最も良く図示したものである。これらの図面中の同じ参照番号及び記号は同じ要素を指すものである。

【図面の簡単な説明】

【００１３】

【図１】デジタル権利管理（ＤＲＭ）コントローラに組み込まれた一実施例を図示している。

【図２】移動する情報についての通信ネットワーク上でのＵＲＬアドレッシングを図示している。

【図３】移動する情報についての通信ネットワーク上でのＵＲＬアドレッシングを図示している。

【図４】ＤＯＩを介した情報へのアクセスを図示している。

【図５】ハンドルの概要を示している。

【図６】ハンドルの概要を示している。

【図７】ユーザーの所望する情報へのアクセスを可能にするための解決メカニズムの概要を示している。

【図８】ユーザーの所望する情報へのアクセスを可能にするための解決メカニズムの概要を示している。

【図９】ユーザーがＤＯＩを用いて情報をアクセスするために行う典型的な一連のアクションの概要を示している。

【図１０】ユーザーが情報の内容をアクセスするために行う典型的な一連のアクションのより完全な概要を示している。

【図１１】通信ネットワーク上で情報をアクセスするための典型的なメカニズムを図示している。

【図１２】通信ネットワーク上で情報を入手するための典型的なメカニズムの別の実施例の概要を図示している。

【図１３】典型的なＤＯＩ登録システムの概要を示している。

【図１４】デジタル・オブジェクト識別子を用いてシステムの耐久性を高める従来のデジタル権利管理シナリオに関わる各者間のインタラクションを図示した機能ブロック図である。

【図１５】ウォーターマークを図１４に示したデジタル権利管理シナリオに組み込むことを図示した機能ブロック図である。

【図１６】図１６Ａは、図１５に示したウォーターマーキング・プロセスの一実施例のフ

ロー図で、結果としてユーザーは保護されたデジタル・ワークを開く。図１６Ｂは、図１５に示したウォーターマーキング・プロセスの一実施例のフロー図で、結果としてユーザーはハッキングされたデジタル・ワークにアクセスする。図１６Ｃは、図１５に示したウォーターマーキング・プロセスの一実施例のフロー図で、結果としてユーザーは非公式に流通されたデジタル・ワークにアクセスする。

【図１７】有効性確認アーキテクチャを図１４に示したデジタル権利管理シナリオに組み込むことを図示した機能ブロック図である。

【図１８】インタラクティブ・インターフェース多重解決メニュー・ファシリティ（ＭＲＭＦ）の非限定的な例を図示した概略図である。

【図１９】インタラクティブ・インターフェース多重解決メニュー・ファシリティ（ＭＲＭＦ）の非限定的な例を図示した概略図である。

【発明を実施するための最良の形態】

【００１４】

［デジタル権利管理コントローラ］

図１は、デジタル権利管理システム（ＤＲＭＳ）コントローラ１０１に取り入れられた一実施例を図示している。この実施例では、ＤＲＭコントローラ１０１はハンドルと関連する全ての情報及び／またはその他の登録、解決、処理、保存、更新及び有効性確認の役割を担う。

一実施例において、ＤＲＭコントローラ１０１は、例えばユーザー入力デバイス１１１、周辺デバイス１１２、通信ネットワーク１１３及び／またはその他からの一人以上のユーザー等のエンティティと接続及び／または通信することができるが、エンティティはこれらに限定されるものではない。ＤＲＭコントローラ１０１は、暗号プロセッサ・デバイス１２８とさえも接続及び／または交信することが可能である。

【００１５】

ＤＲＭコントローラ１０１は典型的には、メモリ１２９及び／またはその他に接続されたコンピュータの系統的システム１０２等の部品から成る一般的なコンピュータ・システムに基づくものであるが、部品はこれに限定されるものではない。

［従来のコンピュータの系統的システム］

従来のコンピュータの系統的システム１０２はクロック１３０、中央演算処理装置（ＣＰＵ）１０３、読み出し専用メモリ（ＲＯＭ）１０６、ランダム・アクセス・メモリ（ＲＡＭ）１０５、インターフェース・バス１０７及び／またはその他から成る。従来は、必ずしもというわけではないが、従来のコンピュータの系統的システム１０２を構成する要素は全てシステム・バス１０４を介して相互接続及び／または交信している。クロック１３０は通常水晶発振器を有し、基本信号を供給する。クロック１３０は通常システム・バス１０４及びコンピュータの系統的システムに取り入れられた他の部品の基本動作周波数を増加させたり減少させたりする様々な手段に結合している。クロック１３０及びコンピュータの系統的システムの様々な部品は、システム内全てにおいて情報を具現する信号を駆動する。コンピュータの系統的システム内において情報を具現する信号のこのような送信及び受信は、通常、通信と呼んでいる。これらの通信に関する信号は、更に、本コンピュータの系統的システムを超え通信ネットワーク、入力機器、他のコンピュータの系統的システム、周辺機器及び／またはその他へ、送信、受信してもよく、返信信号及び／または応答信号を生じさせてもよい。オプションとして、暗号プロセッサ１２６を同様にシステム・バス１０４に接続することもできる。理解されるべきことは、上記の部品の何れもお互いに直接接続したり、ＣＰＵ１０３に接続したり及び／または様々なコンピュータ・システムにより体現されるような数多くのバリエーションで組織化したりしてもよい。

ＣＰＵ１０３はユーザー及び／またはシステムにより出されたリクエストを実行するためのプログラム・モジュールの実行に適した少なくとも一つの高速データ・プロセッサから成る。ＣＰＵ１０３は、インテル社のペンティアム・プロセッサ及び／またはその他のようなマイクロプロセッサでもよいが、これに限定されるものではない。ＣＰＵ１０３は導電性の経路を介して送信される信号を介してメモリと交信し、保存されているプログラム

・コードを実行する。そのような信号送信は、様々なインターフェースを通じてＤＱＡＳコントローラ内の通信及びＤＱＡＳコントローラの域を越える通信を可能にする。

［インターフェース・アダプター］

インターフェース・バス１０７は数多くのインターフェース・アダプターを受け入れ接続し、及び／または通信し、必ずしもアダプター・カードの形である必要はないが、従来その例として、入出力（Ｉ／Ｏ）インターフェース１０８、記憶インターフェース１０９、ネットワーク・インターフェース１１０及び／またはその他があるが、それらに限定されるわけではない。オプションとして、暗号プロセッサ・インターフェース１２７も同様に、任意にインターフェース・バスに接続してもよい。インターフェース・バスは、インターフェース・アダプター同士の通信を提供すると共に、コンピュータの系統的システムにおける他の部品への通信を提供する。インターフェース・アダプターは、コンパチブル・インターフェース・バスに適応している。インターフェース・アダプターは従来、スロット・アーキテクチャを通じてインターフェース・バスに接続する。アクセラレイテッド・グラフィックス・ポート（ＡＧＰ）、カード・バス（拡張）、業界標準アーキテクチャ（（Ｅ）ＩＳＡ）、マイクロ・チャネル・アーキテクチャ（ＭＣＡ）、Ｎｕバス、ペリフェラル・コンポーネント・インターコネクト（ＰＣＩ）、ＰＣメモリ・カード国際協会（ＰＣＭＣＩＡ）及び／またはその他の、従来のスロット・アーキテクチャを用いればよいが、これらに限定されるわけではない。

記憶インターフェース１０９は、例えば記憶装置１１４、リムーバブル・ディスク・デバイス及び／またはその他といった数多くの記憶装置を受け入れ通信し、及び／または接続するが、記憶装置はそれらに限定されるわけではない。記憶インターフェースは、例えば（ウルトラ）アドバンスト・テクノロジー・アタッチメント（パケット・インターフェース）（（ウルトラ）ＡＴＡ（ＰＩ））、（拡張）インテグレイテッド・ドライブ・エレクトロニクス（（Ｅ）ＩＤＥ）、電気電子技術者協会（ＩＥＥＥ）１３９４、ファイバー・チャネル、小型コンピュータ用周辺機器インターフェース（ＳＣＳＩ）、ユニバーサル・シリアル・バス（ＵＳＢ）及び／またはその他といった接続プロトコルを用いるが、これらに限定されるわけではない。

【００１６】

ネットワーク・インターフェース１１０は、通信ネットワーク１１３を受け入れ通信し、及び／または、接続する。ネットワーク・インターフェースは、例えば直接接続、イーサネット（厚型、薄型、ねじれペア１０／１００／１０００ベースＴ及び／またはその他）、トークン・リング、ＩＥＥＥ８０２．１１ｂ等のワイヤレス接続、及び／またはその他といった接続プロトコルを用いるが、これらに限定されるわけではない。通信ネットワーク１１３は、以下に挙げるものの一つ及び／またはそれらの組み合わせである。即ち、ダイレクト・インターコネクション、インターネット、ローカル・エリア・ネットワーク（ＬＡＮ）、メトロポリタン・エリア・ネットワーク（ＭＡＮ）、インターネット上のノードとしてのオペレーティング・ミッション（ＯＭＮＩ）、安全化されたカスタム・コネクション、ワイド・エリア・ネットワーク（ＷＡＮ）、ワイヤレス・ネットワーク（例えば、ワイヤレス・アプリケーション・プロトコル（ＷＡＰ）、Ｉモード及び／またはその他等のプロトコルを用いるが、これに限定されるわけではない）及び／またはその他である。ネットワーク・インターフェースは、入出力インターフェースの特別な形態であると見なされる。

【００１７】

入出力インターフェース（Ｉ／Ｏ）１０８は、ユーザー入力デバイス１１１、周辺機器１１２、暗号プロセッサ・デバイス１２８及び／またはその他を受け入れ通信し、及び／または接続する。Ｉ／Ｏは、例えばアップル・デスクトップ・バス（ＡＤＢ）、アップル・デスクトップ・コネクター（ＡＤＣ）、アナログ、デジタル、モノラル、ＲＣＡ、ステレオ、及び／またはその他に基づくオーディオ、ＩＥＥＥ１３９４、インフラレッド、ジョイスティック、キーボード、ミディ、オプティカル、ＰＣ　ＡＴ、ＰＳ／２、ラジオに基づくパラレル、シリアル、ＵＳＢ、ＢＮＣ、コンポジット、デジタル、ＲＣＡ、Ｓビデオ

、ＶＧＡ、及び／またはその他に基づくビデオ・インターフェース、ワイヤレス及び／またはその他といった接続プロトコルを用いるが、それらに限定されるわけではない。一般的な出力デバイスはビデオ・ディスプレイであり、通常、ビデオ・インターフェースから信号を受け取るインターフェース（例えば、ＶＧＡ回路やケーブル）を有するＣＲＴモニターかＬＣＤモニターから成る。ビデオ・インターフェースは、コンピュータの系統的システムが生み出した情報を合成し、合成された情報に基づいたビデオ信号を生成する。通常、ビデオ・インターフェースは、ビデオ・コネクション・インターフェースを通じて合成されたビデオ情報を提供し、ビデオ・コネクション・インターフェースはビデオ・ディスプレイ・インターフェース（例えば、ＶＧＡディスプレイ・ケーブルを受け入れるＶＧＡコネクター等）を受け入れる。

【００１８】

ユーザー入力デバイス１１１は、カード読み取り装置、ドングル、指紋読み取り装置、手袋、グラフィック・パッド、ジョイスティック、キーボード、マウス（マイス）、トラックボール、トラックパッド、網膜読み取り装置、及び／またはその他といったものである。

【００１９】

周辺機器１１２はＩ／Ｏに、及び／またはネットワーク・インターフェース、記憶インターフェース及び／またはその他といった他のファシリティに接続し、及び／またはそれらと通信したり、またはそれらと交信したりする。周辺機器とは、カメラ、（コピーの防止、デジタル署名としてトランザクションの安全性強化、及び／またはその他のための）ドングル、（追加的な機能としての）外付けプロセッサ、ゴーグル、マイクロフォン、モニター、ネットワーク・インターフェース、プリンター、スキャナー、記憶装置、バイザー及び／またはその他といったものである。

【００２０】

例えばマイクロコントローラ、プロセッサ１２６、インターフェース１２７、及び／またはデバイス１２８のような暗号ユニットをＤＲＭコントローラに付け、及び／または通信してもよいが、暗号ユニットはこれらに限定されるわけではない。通常モトローラ社製であるＭＣ６８ＨＣ１６マイクロコントローラは暗号ユニットとして使用してもよいし、及び／または暗号ユニット内にあってもよい。同等のマイクロコントローラ及び／またはプロセッサを使用してもよい。ＭＣ６８ＨＣ１６マイクロコントローラは、１６ＭＨｚの設定において１６ビットの積算加算インストラクションを活用し、５１２ビットのＲＳＡ秘密鍵機能を実行するために１秒以下しか必要としない。暗号ユニットは交信エージェントからの通信の認証をサポートすると共に、匿名のトランザクションを可能にする。暗号ユニットはまた、ＣＰＵ１０３の一部として設定されていてもよい。他に市販されている専門の暗号プロセッサとしては、ＶＬＳＩテクノロジー社の３３ＭＨｚ６８６８や、セマフォ・コミュニケーション社の４０ＭＨｚのロードランナー２８４がある。

［メモリ］

記憶装置１１４は、従来のコンピュータ・システムの記憶装置のどれであってもい。記憶装置は、固定ハード・ディスク・ドライブ及び／またはその他同類の装置でよい。しかしながら、ＤＲＭコントローラ及び／またはコンピュータの系統的システムは、様々な形態のメモリ１２９を用い得ることは理解されるものである。例えば、コンピュータの系統的システムは、チップ内のＣＰＵメモリ（例えば、レジスタ）、ＲＡＭ、ＲＯＭ、他の記憶装置の機能がパンチ・テープまたは、パンチ・カード・メカニズムによって与えられるように構成されてもよい。もちろん、そのような実施例は好まれるものではなく、動作が極端に遅くなる結果となる。一般的な構成では、メモリ１２９は、ＲＯＭ、ＲＡＭ、記憶装置１１４を含む。通常、プロセッサが情報の記憶及び／または情報の取り出しを実行することを可能にする機械化及び／または実施化は、メモリ１２９と見なされる。それゆえ、コンピュータの系統的システムは一般にメモリを必要とし、メモリを使用する。メモリは、代替可能な技術及びリソースであり、それゆえメモリは任意の数の実施例を代替として利用したり、一緒に利用したりできる。

［モジュール・コレクション］
記憶装置１１４は、プログラム・モジュール及び／またはデータベース・モジュール及び／またはデータといったもののコレクションを含む。それらの例には、オペレーティング・システム・モジュール１１５（即ちオペレーティング・システム）、情報サーバー・モジュール１１６（即ち情報サーバー）、ユーザー・インターフェース・モジュール１１７（即ちユーザー・インターフェース）、ウェブ・ブラウザ・モジュール１１８（即ちウェブ・ブラウザ）、ＤＲＭデータベース１１９、暗号サーバー・モジュール１２０（即ち暗号サーバー）、情報アクセス多重解決サーバー（ＩＡＭＲＳ）モジュール１２５、及び／またはその他（つまり、全体としてモジュール・コレクション）といったものがあるが、それらに限定されるわけではない。これらモジュールは記憶され、記憶装置及び／またはインターフェース・バスを通じてアクセス可能な記憶装置からアクセスできる。モジュール・コレクションにあるような非従来的なソフトウェア・モジュールは一般的に、かつ望ましくはローカル記憶装置１１４に記憶されるが、周辺機器、ＲＡＭ、通信ネットワークを通じた遠隔記憶ファシリティ、ＲＯＭ、様々な形態のメモリ及び／またはその他に取り込み及び／または記憶してもよい。

［オペレーティング・システム］
オペレーティング・システム・モジュール１１５は、ＤＲＭコントローラの動作を可能にする実行可能なプログラム・コードである。一般的に、オペレーティング・システムは、Ｉ／Ｏ、ネットワーク・インターフェース、周辺機器、記憶装置、及び／またはその他のアクセスを可能にする。オペレーティング・システムは、アップル・マッキントッシュＯＳ Ｘ サーバー、ＡＴ＆Ｔ プラン９、マイクロソフト・ウィンドウズＮＴサーバー、ユニックス及び／またはその他のオペレーティング・システムのような従来型の製品が好ましい。好ましくは、オペレーティング・システムは、非常にフォールト・トレラントであり、拡張可能かつ安全であるのがよい。オペレーティング・システムは、モジュール・コレクション内のそのモジュール自体及び／またはその他のファシリティを含む他のモジュールと通信したり、及び／または交信したりする。従来オペレーティング・システムは、他のプログラム・モジュールやユーザー・インターフェース及び／またはその他と通信する。例えば、オペレーティング・システムは、プログラム・モジュール、システム、ユーザー及び／またはデータとの通信、リクエスト及び／またはレスポンスを含み、通信、生成、入手及び／または提供する。オペレーティング・システムは一度ＣＰＵ１０３によって実行されると、通信ネットワーク、データ、Ｉ／Ｏ、周辺機器、プログラム・モジュール、メモリ、ユーザー入力デバイス及び／またはその他とのインタラクションを可能にする。好ましくはオペレーティング・システムは、通信ネットワーク１１３を通じて、ＤＲＭコントローラが他のエンティティと通信できるようにする通信プロトコルを提供する。ハンドル・システムとインタラクションするためのサブキャリア・トランスポート機構として様々な通信プロトコルが、ＤＲＭコントローラによって使用される。通信プロトコルとしては例えばマルチキャスト、ＴＣＰ／ＩＰ、ＵＤＰ、ユニキャスト及び／またはその他といったものがあるが、これらに限定されるわけではない。

［情報サーバー］
情報サーバー・モジュール１１６は、記憶されたプログラム・コードであり、ＣＰＵ１０３により実行される。情報サーバーは、マイクロソフト社のインターネット・インフォメーション・サーバー及び／またはアパッチ・ソフトウェア・ファンデーションのアパッチ等、従来のインターネット情報サーバーでよいが、それらに限定されるわけではない。好ましくは、情報サーバーはＣ＋＋、ジャバ、ジャバスプリクト、アクティブ・エックス、共通ゲートウエイ・インターフェース（ＣＧＩ）スクリプト、アクティブ・サーバー・ページ（ＡＳＰ）及び／またはその他のようなファシリティを通じて、プログラム・モジュールの実行を可能にする。好ましくは、情報サーバーは、安全な通信プロトコルをサポートする。その通信プロトコルは、例えばファイル転送プロトコル（ＦＴＰ）、ハイパーテキスト転送プロトコル（ＨＴＴＰ）、セキュア・ハイパーテキスト転送プロトコル（ＨＴＴＰＳ）、セキュア・ソケット・レイヤー（ＳＳＬ）及び／またはその他であるが、通信

プロトコルはこれらに限定されるわけではない。従来は、情報サーバーは、結果をウェブ・ページの形でウェブ・ブラウザへ提供し、他のプログラムのモジュールとのインタラクションを通じて手を入れられたウェブ・ページの生成を可能にする。ＨＴＴＰリクエストのＤＮＳ解決部分がある特定の情報サーバーへと解決された後、当該情報サーバーは、ＤＲＭコントローラ上の特定された場所情報に対するリクエストを当該ＨＴＴＰリクエストのリマインダーに基づいて解決する。例えば、ｈｔｔｐ：／／１２３／１２４／１２５／１２６／ｍｙＩｎｆｏｒｍａｔｉｏｎ．ｈｔｍｌのようなリクエストは、当該リクエストのＩＰ部分である「１２３／１２４／１２５／１２６」を有しており、それがＤＮＳサーバーによりＩＰアドレスにある一つの情報サーバーへと解決され、するとその情報サーバーが「ｍｙＩｎｆｏｒｍａｔｉｏｎ．ｈｔｍｌ」の部分に対する当該ｈｔｔｐリクエストを更に解析し、それを「ｍｙＩｎｆｏｒｍａｔｉｏｎ．ｈｔｍｌ」の情報を含むメモリの場所へと解決するかもしれない。情報サーバーは、そのモジュール自体及び／またはその他のファシリティを含むモジュール・コレクション内の他のモジュールへと通信したり、及び／またはそれらと交信したりする。情報サーバーが、オペレーティング・システム、他のプログラム・モジュール、ユーザー・インターフェース、ウェブ・ブラウザ及び／またはその他と通信する頻度は非常に高い。情報サーバーは、プログラム・モジュール、システム、ユーザー及び／またはデータとの通信、リクエスト、及び／またはレスポンスを含んだり、通信、生成及び／または入手したりする。

［ユーザー・インターフェース］

ユーザー・インターフェース・モジュール１１７は記憶されたプログラム・コードであり、ＣＰＵ１０３により実行される。好ましくはユーザー・インターフェースは、オペレーティング・システム及び／またはオペレーティング環境によって、あるいはそれらと一緒に、及び／またはそれらの上に与えられる従来型の画像ユーザー・インターフェースであり、システム及び／またはオペレーティング環境とは、例えばアップル・マッキントッシュＯＳ、アクア、マイクロソフト・ウィンドウズ（ＮＴ）、（ＫＤＥ、Ｇｎｏｍｅ及び／またはその他の）ユニックスＸウインドウズ、及び／またはその他である。ユーザー・インターフェースはテキスト・ファシリティ及び／または画像ファシリティを通じて、プログラム・モジュール及び／またはシステム機能を表示、実施、インタラクション、操作及び／またはオペレーションすることを可能にしてもよい。ユーザー・インターフェースは機能を提供するが、その機能とは、ユーザーが、コンピュータのシステムを実行し、インタラクションし及び／または働くものである。ユーザー・インターフェースは、それ自体及び／またはその他の機器を含むモジュール・コレクション内の他のモジュールへと通信及び／またはそれらと交信する。ユーザー・インターフェースがオペレーティング・システムや他のプログラム・モジュール及び／またはその他と通信する頻度は非常に高い。ユーザー・インターフェースは、システム、ユーザー及び／またはデータとの通信、リクエスト、及び／またはレスポンスを含んだり、通信、生成及び／または入手したりする。

［ウェブ・ブラウザ］

ウェブ・ブラウザ・モジュール１１８は記憶されたプログラム・コードであり、ＣＰＵ１０３により実行される。ウェブ・ブラウザは従来のハイパーテキスト・ビューイング・アプリケーションであることが好ましく、例えば、（好ましくは、ＨＴＴＰＳ、ＳＳＬ及び／またはその他のような１２８ビットの暗号化を有する）マイクロソフト・インターネット・エクスプローラーやネットスケープ・ナビゲーターである。ジャバ、ジャバスプリクト、アクティブ・エックス及び／またはその他のようなファシリティを通じて、プログラム・モジュールを実施することが可能なウェブ・ブラウザもある。一実施例では、ウェブ・ブラウザはｗｗｗ．ｃｎｒｉ．ｏｒｇ．から入手可能なハンドル・システム・プラグインのようなブラウザ・プラグイン・ソフトウェアを経てハンドル対応となる。一つの代替実施例においては、ウェブ・ブラウザにハンドル・サポートが組み込まれている。ウェブ・ブラウザやそのような情報アクセス・ツールは、ＰＤＡ、携帯電話及び／または他のモバイル・デバイスに組み込まれていてもよい。ウェブ・ブラウザは、それ自体及びその他のようなファシリティを含むモジュール・コレクション内の他のモジュールと通信したり

、及び／またはと交信する。ウェブ・ブラウザが、情報サービス、オペレーティング・システム、インテグレートされたプログラム・モジュール（例えばプラグ・イン）、及び／またはその他と通信する頻度は非常に高い。例えば、プログラム・モジュール、システム、ユーザー及び／またはデータとの通信、リクエスト、及び／またはレスポンスを含んだり、通信、生成及び／または入手したりするものである。もちろん、ウェブ・ブラウザや情報サーバーの代わりに、両者と同様の機能を持つような複合的なアプリケーションを開発してもよい。複合的なアプリケーションは、ＤＲＭ対応のノードからユーザー、ユーザー・エージェント及び／またはその他への情報の入手および提供を同様に実行する。複合的なアプリケーションは、標準的なウェブ・ブラウザを用いるシステムに対しては役に立たないこともある。安全性を強化するために、そのような複合的なモジュールは、安全性をさらに強化するような中間の情報サーバーが存在しなくても、ＤＲＭと直接通信するように構成することができる。

［デジタル・オブジェクト識別子（ＤＯＩ）］

ＤＯＩはインターネット・プロトコル（ＩＰ）及びその他の場所に基づくアドレス方式の欠点の多くを克服するものである。ＤＯＩは頻繁に移動する可能性のある情報に永続的な識別子を与え、通信ネットワーク上の情報にアクセスすることを可能にする。ＤＯＩは、識別子を場所と関連付けるのではなく、更なるレベルの間接指定を加えて識別子を情報と関連付けるメカニズムを設けることによって、場所をアドレスで指定することに限定されたネットワーク・アドレス方式の限界を克服する。

［ＤＲＭデータベース］

ＤＲＭデータベース・モジュール１１９は、ＣＰＵ１０３により実行される記憶されたプログラム・コードでデータベース内において具現し得て、記憶されたデータであり、記憶された部分のプログラム・コードが記憶されたデータを処理するためのＣＰＵ１０３を設定する。好ましくは、データベースは、例えばオラクルまたはサイベースといった、従来型、フォールト・トレラント、相関的、拡張可能で安全なデータベースであるのがよい。リレーショナル・データベースとは、フラット・ファイルの拡張である。リレーショナル・データベースは、一連の関連し合うテーブルから成る。鍵フィールドを通じてテーブル同士が相互接続する。鍵フィールドの使用によって、鍵フィールドに対するインデキシングによるテーブルの結合が可能になる。つまり、鍵フィールドが様々なテーブルから情報を組み合わせるための、次元的回転軸のような作用をするのである。一般に主要鍵を合わせることによって、相互関係におけるテーブル間に維持されるリンクを識別する。主要鍵は、リレーショナル・データベース内において、テーブルの行を固有に識別するフィールドを表す。より厳密には、主要鍵は、一対多数の関係における「一つの」面にあるテーブルの行を固有に識別するのである。

代わりに、配列、ハッシュ、（リンクした）リスト、ストラクト及び／またはその他の様々な標準的なデータ構造を用いて、ＤＲＭデータベースを実施してもよい。そのようなデータ構造は、メモリ及び／または（構造的な）ファイルに保存してもよい。仮にＤＲＭデータベースをデータ構造として実施すると、ＤＲＭデータベースの使用は例えばＤＲＭモジュールのような他のモジュールに組み込まれ得る。データベースは、標準的なデータ処理技術を介した無数のバリエーションによって、統合及び／または分散される。データベースの一部分、例えばテーブルは、エクスポート及び／またはインポートでき、それによって、分散したり及び／または統合したりする。非限定的な一実施例では、ＤＲＭデータベース１１９は、例えばＵＮＩ（例えばハンドル、ＤＯＩ及び／または他のＵＮＩ）、テーブル１１９ａ、ＵＲＬテーブル１１９ｂ、メタデータ・テーブル１１９ｃ、多重解決テーブル１１９ｄ、ポリシー・テーブル１１９ｅ及び／またはその他といったテーブルを含むが、これらに限定されるわけではない。全てのテーブルは、（強化）ＤＯＩ鍵フィールド・エントリーが固有なので、このエントリーについて関係し得る。別の実施例では、これらのテーブルは、自身のデータベースとそれぞれのデータベース・コントローラ（つまり、上記テーブルそれぞれの個別のデータベース・コントローラ）に分散化されている。もちろん、標準的なデータ処理技術を用いて、データベースを幾つかのコンピュータのシ

ステム的系統及び／または保存装置にわたってさらにデータベースを分散してもよい。同様に、分散したデータベース・コントローラの構成は、様々なデータベース・モジュール１１９ａ－ｅを統合及び／または分散することによって、変えることができる。ＤＲＭデータベース１１９は、データベース・コントローラを通じたユーザーのリクエスト及び様々なトランザクションを追跡するように構成してもよい。

【００２１】

ＤＲＭデータベース１１９は、それ自体及び／またはその他のファシリティを含むモジュール・コレクション内の他のモジュールと通信したり、及び／または交信したりする。ＤＲＭデータベース１１９がＤＲＭモジュール、他のプログラム・モジュール及び／またはその他と通信する頻度は非常に高い。データベースは、他のノード及びデータに関する情報を入手し、保持し、提供する。

［暗号サーバー］

暗号サーバー・モジュール１２０とは、保存されたプログラム・コードであり、ＣＰＵ１０３、暗号プロセッサ１２６、暗号プロセッサ・インターフェース１２７、暗号プロセッサ装置１２８、及び／またはその他のものにより実行される。暗号プロセッサ・インターフェースが暗号モジュールにより暗号化及び／または暗号解読のリクエストを迅速に実施することを可能にすることが望ましい。代わりに暗号サーバー・モジュール１２０を従来のＣＰＵに実行させても良い。暗号サーバー・モジュール１２０が、供給されたデータの暗号化及び／または暗号解読を可能にすることが望ましい。暗号サーバー・モジュール１２０が対称及び非対称（例えばＰｒｅｔｔｙ Ｇｏｏｄ Ｐｒｏｔｅｃｔｉｏｎ（ＰＧＲ））双方の暗号化及び／または暗号解読を可能にすることが望ましい。暗号サーバー・モジュール１２０は従来の暗号技術、例えば、デジタル証明（例えば、Ｘ．５０９認証枠組み）、デジタル署名、複式署名、エンベロッピング、パスワード・アクセス保護、公開鍵管理、及び／またはその他のものを可能にすることが望ましいが、従来の暗号技術はそれらに限定されるわけではない。暗号サーバー・モジュール１２０は数々の（暗号化及び／または暗号解読）セキュリティ・プロトコル、例えば、チェックサム、データ暗号化基準（ＤＥＳ）、楕円曲線暗号化（ＥＣＣ）、国際データ暗号化アルゴリズム（ＩＤＥＡ）、メッセージ・ダイジェスト５（ＭＤ５、即ち一方向ハッシュ関数）、パスワード、ＲＣ５（リベスト暗号）、リジンデール、ＲＳＡ（インターネット暗号化及び認証システムで、１９７７年にロン・リベスト、アデイ・シャミル及びレオナルド・エイドウルマンが開発したもの）、セキュア・ハッシュ・アルゴリズム（ＳＨＡ）、セキュア・ソケット・レイヤー（ＳＳＬ）、セキュア・ハイパーテキスト転送プロトコル（ＨＴＴＰＳ）、及び／またはその他のものを可能にすることが望ましいが、セキュリティ・プロトコルはそれらに限定されるわけではない。暗号モジュールは「セキュリティ許可」のプロセスを可能にし、それによってリソースへのアクセスはセキュリティ・プロトコルにより阻害され、暗号モジュールは安全性を保たれたリソースへの許可されたアクセスを実行する。暗号モジュールはモジュール・コレクション中の他のモジュールと通信及び／または交信してもよく、その中には暗号モジュール自体及び／その他のファシリティも含まれる。暗号サーバー・モジュール１２０は、通信ネットワーク上での情報の安全な送信を可能にする暗号化方式を支援することが好ましく、もしユーザーが希望すれば、ＤＲＭモジュールが安全なトランザクションに用いられ得るようにする。暗号モジュールは、ＤＲＭ上のソースの安全なアクセスを可能にするが、つまり安全化されたソースのクライアント及び／またはサーバーとして機能する。暗号サーバー・モジュール１２０が情報サーバー、オペレーティング・システム、その他のプログラム・モジュール及び／またはその他のものと交信する頻度は非常に高い。暗号サーバー・モジュール１２０はプログラム・モジュール、システム、ユーザー及び／またはデータとの通信、リクエスト、及び／またはレスポンスを含み、通信、生成、入手及び／または提供する。

［情報アクセス多重解決サーバー（ＩＡＭＲＳ）］

ＩＡＭＲＳモジュール１２５は保存されたプログラム・コードであり、ＣＰＵ１０３により実行される。一般にＤＲＭは、通信ネットワーク上のノード間における情報のアクセス

、入手、提供、及び／またはその他を実行する。ＩＡＭＲＳはＵＮＩを、入ってくるリクエストのタイプに応じて多重のインスタンス化及びサービスへと解決する能力を有している。一般に、ＩＡＭＲＳはルックアップ機能として役を果たし、与えられた情報、そのＤＯＩ、その現在の場所及び関連するサービスへのポインターとの間の関連性の作成、維持、登録、及び更新を行う。ＩＡＭＲＳはＤＲＭデータベースと提携して、リクエストされた情報のデータ転送の向上、リクエストされた情報の種々のフォーマットへの解決、情報についてのクエリー作成用の強化されたメカニズムの提供及び／またはその他に役立つと思われるノードを識別する。ＩＡＭＲＳによるノード間の情報アクセス可能化の開発にあたっては、標準開発ツールを使用してもよい。例えば、Ｃ＋＋、シェル・スクリプト、ジャバ、ジャバ・スクリプト、ＳＱＬコマンド、ウエブ・アプリケーション・サーバー・エクステンション、アパッチ・モジュール、パール・スクプリト、バイナリ・エクセキュータブル、及び／またはその他のマッピング・ツール及び／またはその他を用いることができるが、標準開発ツールはそれらに限定されるわけではない。一つの非限定的な実施例においては、ＩＡＭＲＳサーバーは暗号化サーバーを用いて通信の暗号化及び暗号解読にあたっている。ＩＡＭＲＳはリクエストのサービス、ＵＮＩのための関連性情報の更新、その他多くのことにあたることができる。ＤＲＭモジュールはモジュール・コレクション中の他のモジュールと通信及び／または交信してもよく、その中にはＤＲＭモジュール自体及び／またはその他のファシリティも含まれる。ＩＡＭＲＳモジュールがＤＲＭデーターベース、オペレーティングシステム、その他のプログラム・モジュール及び／またはその他と交信する頻度は非常に高い。ＩＡＭＲＳはプログラムモジュール、システム、ユーザー及び／またはデータとの通信、リクエスト、及び／またはレスポンス等を含み、通信、生成、入手及び／または提供する。

［デジタル権利管理サーバー（ＤＲＭＳ）］

ＤＲＭモジュール１３５は保存されたプログラム・コードであり、ＣＰＵ１０３により実行される。ＤＲＭモジュール１３５は、情報アクセス登録システム（ＩＡＲＳ）のようなＵＮＩ登録システムからは分離して独立モードで動作可能である。ＤＲＭモジュール１３５は、情報の有効性を確認できるようにＤＯＩによって表される情報に組み込まれたタグを生成することができる。ＤＲＭモジュール１３５は、ＤＲＭデータベースと提携して、ＵＮＩと関連する情報の完全性の有効性の確認、リクエストされた情報のデータ転送の向上、リクエストされた情報の種々のフォーマットへの解決、情報についてのクエリー作成用の強化されたメカニズムの提供及び／またはその他に役立つと思われるノードを識別する。ＤＲＭによるノード間の情報アクセス可能化の開発にあたっては、標準開発ツールを使用してもよい。例えば、Ｃ＋＋、シェル・スクリプト、ジャバ、ジャバ・スクリプト、ＳＱＬコマンド、ウエブ・アプリケーション・サーバー・エクステンション、アパッチ・モジュール、パール・スクプリト、バイナリ・エクセキュータブル、及び／またはその他のマッピング・ツール及び／またはその他を用いることができるが、標準開発ツールはそれらに限定されるわけではない。一つの非限定的な実施例においては、ＤＲＭモジュール１３５は暗号サーバーを用いて通信の暗号化及び暗号解読にあたっている。ＤＲＭモジュール１３５は、リクエストのサービス、リクエストのリダイレクト、ＵＮＩのための関連性情報の更新、その他多くのことにあたることができる。ＤＲＭモジュール１３５は、モジュール・コレクション中の他のモジュールと通信及び／または交信してもよく、その中にはＤＲＭモジュール１３５自体及び／またはその他のファシリティも含まれる。ＤＲＭモジュール１３５がＤＲＭデーターベース、ＩＡＭＲＳモジュール、ＩＡＲＳモジュール、オペレイティングシステム、その他のプログラム・モジュール及び／またはその他と交信する頻度は非常に高い。ＤＲＭモジュール１３５はプログラムモジュール、システム、ユーザー及び／またはデータとの通信、リクエスト、及び／またはレスポンス等を含み、通信、生成、入手及び／または提供する。

［分散型ＤＲＭＳ］

ＤＲＭノード・コントローラの構成要素は何れもあらゆる方法で、その機能性を組み合わせ、統合及び／または分散することが可能であり、開発及び／または配備を可能にするこ

とができる。同様に、モジュール・コレクションも開発及び／または配備を可能にすべくあらゆる方法で組み合わせることができる。これを達成するには、単に各構成要素を共通のコード・ベースに統合するか、あるいは必要に応じて統合的に構成要素をダイナミックにロードできるファシリティに統合すれば良いのである。

【００２２】

モジュール・コレクションを統合及び／または分散するにあたっては、標準的なデータ処理及び／または開発技術を介した無数のバリエーションがある。プログラム・モジュール・コレクション中の何れのプログラムの多重のインスタンスをも単一のノードでインスタンス化でき、及び／または負荷バランシング・データ処理技術を通し、多数のノードを使用し性能を向上することもできる。更に、単一のインスタンスもまた複数のコントローラ及び／または記憶装置、例えばデータベースに分散することができる。

【００２３】

全てのプログラム・モジュールのインスタンスとコントローラは、標準的なデータ処理通信技術を通じ、共同作業を行う。

【００２４】

好ましいＤＲＭコントローラの構成は、システム配備のコンテキストによって異なる。例えば、元となるハードウェア・リソースの能力及び／または場所等のファクターが配置条件や構成に影響するが、こうしたファクターはそれらに限定されるわけではない。例え構成がプログラム・モジュールを合同及び／または統合する結果になろうが、分散化されたプログラム・モジュールより成り立つ結果になろうが、及び／または統合型と分散型の何らかの組み合わせになろうが、データの通信にあたっては、通信、入手、提供が可能である。プログラム・モジュール・コレクション中からの共通コード・ベースに統合された（モジュール・コレクション中の）モジュールのインスタンスは、データの交信、入手及び／または提供にあたることができる。これは、例えば、データ・レファレンシング（例えば、ポインタ等）、内部メッセージ、オブジェクト・インスタンス可変通信、共有メモリ・スペース、可変パッシング及び／またはその他のもの（アプリケーション内部の通信）等の基準データ処理技術を用いることにより達成されるが、これらに限定されるわけではない。

もしモジュールコレクションの構成要素がお互いに個別的、分離的、及び／または外部的である場合は、データの通信、入手、及び／または提供を他のモジュール構成要素と行う及び／または他のモジュール構成要素へと行うにあたっては、標準的なデータ処理技術を用いればよい。標準的なデータ処理技術には例えば、アプリケーション・プログラム・インターフェース（ＡＰＩ）情報パッセージ；（分散型）コンポーネント・オブジェクト・モデル（（Ｄ）ＣＯＭ）、（分散型）オブジェクト・リンキング・アンド・エンベディング（（Ｄ）ＯＬＥ）、及び／またはその他のもの）、コモン・オブジェクト・リクエスト・ブローカー・アーキテクチャー（ＣＯＲＢＡ）、プロセス・パイプ、共有ファイル及び／またはその他のもの（アプリケーション間の通信）があるが、これらに限定されるわけではない。グラマーの生成及び解析は、アプリケーション間の通信のための個別のモジュールの構成要素間で送ったメッセージや、アプリケーション内部の通信のための単一モジュールにおけるメモリ空間内で送ったメッセージを促進する。グラマーは、例えばｌｅｘ、ｙａｃｃ及び／またはその他といった標準的な開発ツールを使用して開発してもよい。それらの標準的な開発ツールは、グラマーの生成及び機能性の解析を可能にし、これらは今度はモジュール内及びモジュール間の通信メッセージの基礎を形成する。この場合もまた、好ましい実施例はシステム配備のコンテキスト次第である。

【００２５】

最後に、モジュール・コレクションの如何なる組み合わせ及び／または図と全体に渡って説明される本発明の如何なる組み合わせにおける論理上な構造及び／またはトポロジー構造は、固定された実施順位及び／またはアレンジメントに限定されるわけではなく、むしろ、開示した順位は典型的なものであり、順位にかかわらず全て機能的に等価であるものを本開示は意図していることを理解すべきである。更に、そのような構造は連続実行に限

定されるものではなく、むしろ、非同期的に、同時的に、同期的に及び／またはその他に実行できる如何なる数のスレッド、プロセス、サービス、サーバー及び／またはその他を本開示は意図していることにも注意すべきである。

［ＩＰアドレッシング］

ユーザーはアドレスを介して通信ネットワークにアクセスする。アドレスは場所を表している。ユーザーは通信ネットワークにおいて、情報を探し出すべく場所から場所へ移動する。一般的な通信アドレス方式はＩＰアドレスを用いている。ＩＰアドレスは現実の世界では住所に例えることができる。ＩＰアドレス自体は、例えば２０９．５４．９４．９９といった一連の数字であり、通常は、例えばｗｗｗ．ｃｏｎｔｅｎｔｄｉｒｅｃｔｉｏｎｓ．ｃｏｍというような関連する名前を有する。分散型データベース・レジストリは名前とＩＰアドレスの関連するペアを維持し、関連する名前を対応するＩＰアドレスへと解決する役目を担う。これにより、ユーザーは、２０９．５４．９４．９９といった一連の数字を暗記して用いる代わりに、例えばｗｗｗ．ｒｅｐｏｒｔ．ｃｏｍといった名前を覚えておいて使用することが可能になる。ＩＰアドレスの名前解決を支援するこれらの分散型データベースは、一般的にドメイン・ネーム・サーバー（ＤＮＳ）と呼ばれている。

【００２６】

ＩＰアドレスを、アドレスに更なるナビゲーション情報を付加したユニバーサル・リソース・ロケーター（ＵＲＬ）として具現することが一般的である。ユーザーは、ＨＴＴＰを用いてＵＲＬに保存されている情報をアクセスするためにソフトウェアを用いてもよい。一例を挙げると、ユーザーが「ｈｔｔｐ：／／ｗｗｗ．ｒｅｐｏｒｔ．ｃｏｍ／ｒｅｐｏｒｔｓ／１９９９／ＩｎｃｏｍｅＳｔａｔｅｍｅｎｔ．ｈｔｍｌ」とウェブ・ブラウザに指定する。すると通常この更なるナビゲーション情報である「／ｒｅｐｏｒｔｓ／１９９９／ＩｎｃｏｍｅＳｔａｔｅｍｅｎｔ．ｈｔｍｌ」がコンピュータ・サーバー内の特定の保存場所を提示する。この更なるナビゲーション場所は、現実の世界では番地よりも詳しい、会社名や部署名、部屋番号等を含む住所に例えることができる。この更なるナビゲーション場所の取り扱いや解決は、通常ＤＮＳではなく解決されたＩＰアドレスにある情報サーバーにより行われる。例えば、ｗｗｗ．ｒｅｐｏｒｔ．ｃｏｍに対して解決したアドレスである１２３．１２３．１２３．１２３にある情報サーバーは、サーバー内のローカルの場所「／ｒｅｐｏｒｔｓ／１９９９／ＩｎｃｏｍｅＳｔａｔｅｍｅｎｔ．ｈｔｍｌ」にある情報を解釈し返送する。情報サーバーとは、通信ネットワークと特定のＩＰアドレスにあるコンピュータ・サーバーの間の通信を可能にする手段である。情報サーバーの商業的な例としては、アパッチが挙げられる。情報サーバーは、企業内の該当部署へ郵便物を仕分ける企業のメール室に例えることができる。

図２と図３は、ＩＰアドレッシング・メカニズムは、情報が通信ネットワーク上で移動する間に、情報との関連を維持しないということを図示している。一般的にウェブ・ページのリンクにはＨＴＴＰを用い、ＨＴＴＰはＩＰアドレッシングに依存している。従って、ＵＲＬリンクは単に通信ネットワーク上の場所を示すだけで、必ずしも特定の情報と関連しているわけではない。例えば、ｗｗｗ．ｎｅｗｓ．ｃｏｍをレファレンスするＵＲＬリンクによってＵＲＬとｗｗｗ．ｎｅｗｓ．ｃｏｍで入手可能な情報を関連付けてもたらされる情報は、その場所では毎日情報が更新されるため、異なる情報となる。多くの場合、企業が情報を移動させたり、事業を移動させたり、廃業したりすると、場所そのものが消失する。

【００２７】

例えば、ｗｗｗ．ｒｅｐｏｒｔ．ｃｏｍ／１９９９／Ｒｅｐｏｒｔ．ｈｔｍｌ２０８という場所に存在した「１９９９年度売り上げ」というタイトルのレポート２２２が、当該情報があるエンティティから別のエンティティに売られたり、アーカイブされたり、あるいはその他様々な理由で、例えばｗｗｗ．ｒｅｐｏｒｔ－ａｒｃｈｉｖｅｓ．ｃｏｍ／１９９９／Ｏｌｄ－ｒｅｐｏｒｔ．ｈｔｍｌ３１０という場所に移動することもある。ｗｗｗ．ｒｅｐｏｒｔ．ｃｏｍ／１９９９／Ｒｅｐｏｒｔ．ｈｔｍｌ２０８という場所に存在したレポートは５００万ウェブ・ページ及び場所２４４をレファレンスするＵＲＬリンクを

有したかもしれず、ユーザーが当該情報へのアクセスを試みると、その場所は既に存在しないため及び／またはその場所はユーザーが所望した情報を含まないため、ユーザーは「４０４Ｆｉｌｅ　ｎｏｔ　ｆｏｕｎｄ」のエラー３０９を受け取る可能性もある。結果としてエラーが出るのは、ＤＮＳは常にユーザーのリクエストを場所へと解決するよう設計されているためであり、またＤＮＳはＵＲＬと特定の情報のインスタンス化との関連を維持するように設計されていないためである。

図２はウェブ・ページ２０１、ユーザーが入力したアドレス２０２、ドキュメント２０３及びメモリ・デバイス２０４を描写し、それぞれ一つの情報（「１９９９年度売り上げ」のレポート２２２）をレファレンスするためにＵＲＬを、従ってＩＰアドレッシングを用いる。次に図２では、情報２２２は元の場所２０８（例えば、ｗｗｗ．ｒｅｐｏｒｔ．ｃｏｍ／１９９９／Ｒｅｐｏｒｔ．ｈｔｍｌ）から図３の新しい場所３１０（例えばｗｗｗ．ｒｅｐｏｒｔ．ｃｏｍ／１９９９／Ａｒｃｈｉｖｅｓ．ｈｔｍｌ）へ移動する。図３において、この結果として当該の場所をレファレンスする全てのＵＲＬ２４４のブレーキング３０１－３０４が起こり、あの恐ろしい「４０４Ｆｉｌｅ　ｎｏｔ　ｆｏｕｎｄ」のエラー３０９を、当該の場所（ｗｗｗ．ｒｅｐｏｒｔ．ｃｏｍ／１９９９／Ｒｅｐｏｒｔ．ｈｔｍｌ）２０８へレファレンスする全てのユーザーとＵＲＬに提示することになる。

【００２８】

［ハンドル・システム］

ひとたび一つの情報にＤＯＩが指定され利用可能になると、ＤＯＩシステムはＤＯＩのユーザーがアクセスを望むものを解決できるようになる必要がある。ＤＯＩの解決を成し遂げるために用いる技術は、「ハンドル・システム」としてより広く知られており、以下により詳しく説明する。ＤＯＩハンドブックには基本的なＤＯＩの一般的な概要が記載されている。一言で言えば、ハンドル・システムはプロトコルのオープンなセット、ネームスペース及びプロトコルの実施化を含む。プロトコルは分散型コンピュータ・システムが、デジタル・コンテンツのハンドル（ＤＯＩ等）を保存し、コンテンツの所在を確認しアクセスするため、当該コンテンツに関係する情報の所在を確認しアクセスするため、あるいは当該コンテンツに関連するサービスの所在を確認しアクセスするために（即ちそのようなサービスへのインターフェースを提供するために）必要な情報へと、それらのハンドルを解決することを可能にする。必要に応じて、ＤＯＩを変更することなく識別されたコンテンツの現状を反映するために、この関連情報を変更することができるので、場所やその他の状況の情報の変更を経てもアイテムの名前が存続することが可能になる。一元管理されたＤＯＩ登録機関と共に、ハンドル・システムは長期にわたるネットワーク上の情報及びサービスの信頼性のある管理のための、汎用且つ分散型のグローバル・ネーミング・サービスを提供する。本開示全体にわたり、ＤＯＩシステムを介してアクセス可能になった「ソース」、「コンテンツ」及び／または「情報」とは、特定が可能な全てのコンテンツ、ソース、情報、サービス、トランザクション及び記事、書籍、無形オブジェクト、音楽アルバムを含む著作物、人物、有形で物理的なオブジェクト、その他及び／またはそれらの選択された個別の部分及び／またはそれらの組み合わせを更に含む、から成り得ることに注意することが重要である。アクセス可能な情報は、サービスやトランザクションを開始するアプリケーションや、選択のメカニズム及び／またはその他を提供するアプリケーション等へのＵＲＬでもよい。一つの非限定的な例では、ＤＯＩは、ソーシャル・セキュリティ番号、電話番号及び／またはその他のある人物を識別する情報と関連付けられることすらあり得る。別の非限定的な例においては、ＤＯＩはソフトウェア・モジュール、プログラミング「オブジェクト」またはその他のネットワークに基づくリソースの何かと関連付けられたりもする。更に、実際の製品（現在ＵＰＣやバーコードで識別されている品物等）のオンラインでの表示を含むほとんど全てのものを表示するためにＤＯＩを用いることができる。そのような例では、ＤＯＩはある製品を説明したり販売したりしている製造者のカタログ・ページへと解決することができ、多重解決シナリオにおいては、ある品物を修理してもらうにはどこへ行けばよいか、交換用の部品はどこへ行けば見つかるか、新製品あるいは交換用の製品はどのようなものか、どのような価格またはリースのオプシ

ョンがあるのか等、当該オブジェクトに関係する全てのサービスへと解決することができる。ＤＯＩを実施するその他の実施例に含まれるのは、通信ネットワークを介して分散型の方法で動作することができるソフトウェアの異なるモジュールの表示、ボイス・オーバーＩＰ技術のための電話番号、遺伝子配列、医療記録及び／またはその他の恒久的な記録（ＤＯＩは、サーティフィケートあるいは暗号解読鍵を呼び出すこともある暗号化及び／またはその他の方法で保護された恒久的な記録に特に有用）及び／または同様のもの、である。別の実施例ではＤＯＩは、例えば現在の株価、（株及び／またはその他全てのオークション及び／または為替の）最新の競売価格や売り出し価格、（別の過去の年次報告書には異なるＤＯＩが割り当てられているのに対して）企業の最新の年次報告書、及び／またはその他のようなもので、しかしこれらに限定されない一時的及び／または動的なバリューの恒久的な場所を表す。

ユーザーはデジタル・オブジェクト・アイデンティファイアー（ＤＯＩ）を介して情報にアクセスし得る。ＤＯＩは情報そのものに関連付けられている（即ち情報自体の名前である）。ＤＯＩは「ハンドル」のインスタンスであり、「ハンドル・システム」の枠組みの中で動作する。ＤＯＩは永続的に関連付けられた情報へのアクセスを可能にする。ＤＯＩは、一連の文字の後にセパレーターが付き、その更に後に一連の文字が付いたもので、例えば１０．１０６５／ａｂｃ１２３ｄｅｆというようになる。注意すべき、そして再び強調すべきことは、本開示は「ＵＲＮ」「ＤＯＩ」「ハンドル」といったＵＮＩの特定のサブ・タイプについて記載することもあるが、本開示はより一般的なタイプのＵＮＩにも同等に適用されるものであり、従って特に断りの無い限り本開示はＵＮＩのあるサブ・タイプに言及する場合はＵＮＩ全般にわたって適用されるものと見做されるべきものである。更に、今日使用されているハンドル・システム、ＤＯＩ及びそれらの支援技術や仕様は、本開示の意図したフォーラムではあるものの、本開示は最新の、または今後考案される仕様やシステムに基づいた他のフォーラムにも応用できることを意図していることに注意すべきである。

［ＤＯＩ］

情報にアクセスするためにＤＯＩを使用しているユーザーは、ＤＯＩが関連付けられた情報のみを解決しアクセスすることを知っている。場所をレファレンスするＵＲＬとは対照的に、ＤＯＩとは情報に対する名前であり、その情報の場所やその他の属性、と共に関係するサービスをも見るために用いることができる。情報とは、電子書籍、音楽ファイル、ビデオ・ファイル、電子ジャーナル、ソフトウェア及び前記のコンテンツの一部及び／またはそれらの組み合わせも含む情報と共にコンピュータで読み取り可能なファイル全てを含むと考えられる。電子コンテンツは通信ネットワーク上で利用可能となっているので、これ以降本出願書はそのような利用可能な情報は、通信ネットワーク上で発行されたものとみなすということに注意されたい。

【００２９】

ＤＯＩは、通信ネットワーク上で利用可能な情報に与えられた恒久的で永続的な識別子で、仮にコンテンツあるいは関連するデータの場所（即ちＵＲＬ）、フォーマット、所有権等が変更されたとしてもユーザーが関連データにアクセスすることができるように、電子的形態で登録されている。ＤＯＩまたはハンドルは、ＵＲＬの代わりにユーザーに配信できる。ユーザーは、ハンドル対応のウェブ・ブラウザに、ＵＲＬハイパーリンクと同様にＤＯＩを選択したり入力したりすることにより、ある特定のＤＯＩに関連付けられた情報にアクセスする。例えばｗｗｗ．ｃｎｒｉ．ｏｒｇから入手可能なハンドル・システム・プラグイン等のブラウザ・プラグイン・ソフトウェアを用いて、数多くの種類のブラウザをハンドル対応にすることが可能である。ＤＯＩに関連付けられた情報にアクセスするためのそのような試みにより、リソースの現在の所在を確認する自動のプロセスが起動する。当該リソースの現在の場所は、ハンドル・システムによって利用可能な一元管理されたディレクトリ内の当該リソースのＤＯＩに関連付けられており、それが今度はユーザーを（即ちユーザーのウェブ・ブラウザを）当該リソースの現在の場所へと導く。この誘導はしばしば、選択されたＤＯＩに関連する現在のＵＲＬと、対応する情報を返信することに

よって実行される。
図４はＤＯＩを介した情報へのアクセスを上記の図２及び図３と対比して図示している。最初に、登録プロセスを経て情報（「１９９９年度売り上げ」のレポート２２２）にＤＯＩが与えられる。ＵＲＬを用いる代わりに、ユーザーはＤＯＩを用いウェブ・ページ４０１、ウェブ・ブラウザへのタイプ入力４０２、ドキュメント４０３、デバイス４０４、バーコード４０６及び／またはその他を介して当該情報のレファレンス４４４を行う。ユーザーがＤＯＩリンク４４４を行うと、それらは一元管理されたＤＯＩディレクトリ４１１において解決され、リクエストしたユーザーは情報２２２の最初の場所（ｗｗｗ．ｒｅｐｏｒｔ．ｃｏｍ／１９９９／Ｒｅｐｏｒｔ．ｈｔｍｌ２０８）へのＵＲＬリンク２４４を与えられる。当該情報が最初の場所（ｗｗｗ．ｒｅｐｏｒｔ．ｃｏｍ／１９９９／Ｒｅｐｏｒｔ．ｈｔｍｌ２０８）から新たな場所（ｗｗｗ．ｒｅｐｏｒｔ．ｃｏｍ／１９９９／Ａｒｃｈｉｖｅｓ．ｈｔｍｌ３１０）へ移動４３４すると、当該情報の発行者４１０は新たな場所をレファレンスする更新されたＵＲＬ２４５を送ることにより、ＤＯＩ一元管理ディレクトリ４４５に当該情報の新しい場所を知らせる。それ以降、ユーザー４０１－４０４がＤＯＩリンク４４４を介して当該情報にアクセスを試みると、ＤＯＩディレクトリは更新されたＵＲＬ２４５を通して適正に新しい場所３１０を提示する。
【００３０】
上記のように、ＤＯＩは情報のみならず、その一部を識別するために用いることもできる。例えば、ＤＯＩシステムによれば、１冊の書籍が一つのＤＯＩを有することが可能な一方、その書籍のそれぞれの章が別の、それぞれの章を識別するための固有のＤＯＩを有することもあり、更にはその書籍中の図面一つ一つがそれら図面を識別するための固有のＤＯＩを有することも可能である。言い換えれば、ＤＯＩシステムによると、コンテンツ発行者の希望通りに様々な細かさのデータの塊として情報を識別することができる。なお、ユニバーサル・プロダクト・コード（一般的には消費者向け製品の「バーコード」として表示されている）によって例えば、スーパーのレジ、在庫コンピュータ、財務システム及び流通業者が現実の世界でサプライ・チェーンを自動化することが可能になるように、本開示はＤＯＩを用いて世界中の全ての電子発行エージェントがインターネットを介したデジタル・コンテンツ（及びそのコンテンツに対する権利のライセンス）の販売を効率的な方法で自動化することを可能にするメカニズムを提供すると想定している。何故ならば、販売可能なコンテンツのそれぞれが世界で唯一のＤＯＩを有しており、それをエージェント同士のトランザクションにおいて製品の識別コードとして使用することが可能だからである。
［ハンドル構造］
ハンドル・システムは、効率的でユーザーに分かり易い利用を可能にするための前もって決められた方針の一群を採っており、そのうち幾つかを以下に挙げる。発行者がオペレーション・コストを負担して、ＤＯＩ解決のためのハンドル・システムの使用がユーザーには無料となるのが理想的である。ＤＯＩは全て世界的なＤＯＩ機関に登録される。登録者は、登録したＤＯＩに関する状態データ及びメタデータを維持する責任がある。ＤＯＩのシンタックスは標準化されたシンタックスに準じる。使用にあたっては、ＤＯＩはオペーク・ストリング（ダム・ナンバー）になる。ＤＯＩ登録機関はＤＯＩの指定、登録、ＤＯＩに関連するメタデータの申告を管理する。
【００３１】
図５及び図６は、ハンドル６００の概略図である。ハンドル６００は二つの構成要素である、プレフィックス５０１とサフィックス５０２を有する。プレフィックス５０１とサフィックス６０２は、フォワード・スラッシュ５０７により区切られている。ハンドル５００には、印刷できる文字であれば、今日書かれたり使用されたりしているほとんど全ての主要な言語のどれを取り入れてもよい。プレフィックス５０１にもサフィックス５０２にも特に長さの制限はない。結果として、利用可能なハンドルの数はほとんど無限であると想定される。プレフィックス５０１とサフィックス５０２の組み合わせを確実に唯一固有なものにすることが、ハンドル・システムの完全性を維持するためには重要である。その

ため、ＤＯＩ登録機関は発行者に固有のプレフィックス５０１を与え、一実施例ではその登録機関が、指定するサフィックス５０２もまた確実に固有のものであるようにする責任を発行者に課す。これはユーザーのクライアント・コンピュータ・システム上で動作している登録ツールによって達成され得る。別の実施例では、本開示全体にわたって記載しているように、様々なサフィックス生成アルゴリズムを適用することによって、登録機関がサフィックス５０２が固有なものもであること確実にする。登録機関とハンドル・システム管理者は共に、新しいハンドルについては全てその固有性を確認してからハンドル・システムに入れる。登録機関はハンドル・システムにＤＯＩ記録を入れ、それを受けてハンドル・システムはＤＯＩディレクトリを介してＤＯＩ解決リクエストに対し情報を提供する。

プレフィックス５０１自体は、プレフィックス・セパレーター５０６、即ちピリオドにより区切られる二つの構成要素を有する。ハンドル・プレフィックスの第一の部分はハンドル・タイプ５０４で、第二の部分はハンドル・クリエーター５０５である。ハンドル・タイプ５０４は、どのようなタイプのハンドル・システムが使用されているかを識別する。ハンドル・タイプ５０４が「１０」で始まる場合、当該ハンドルはＤＯＩであると識別され、ハンドル・システムの他の実施タイプではないと分かる。ピリオドにより区切られたプレフィックスの次の要素であるハンドル・クリエーター５０５は、ＤＯＩの登録を希望する団体に与えられる番号（または文字列）である。これら二つの要素５０４と５０５が一緒になり、ＤＯＩの固有の発行者プレフィックス部分を形成する。どの団体が申請するハンドル（より詳しくはＤＯＩ）プレフィックスの数にも制限はない。結果として、例えば出版社は一つのＤＯＩプレフィックス５０１を有してもよいし、ジャーナルごとに異なるプレフィックスを有することも、そのジャーナルの刷り込み毎に一つのプレフィックスを有することもできる。通常プレフィックス５０１は単純な数字列だが、ハンドル・システムの範囲はそれに限定されるものではない。従って、プレフィックス５０１にアルファベットやその他の文字を用いてもよい。

サフィックス５０２は固有の英数字列であり、特定のプレフィックスと共に、固有情報を識別する。発行者のプレフィックス５０１と発行者の提示する固有のサフィックス５０２の組み合わせにより、ＤＯＩ番号の一元割り当ての必要性を免れる。サフィックス５０２は、当該発行者がプレフィックスと共に登録した他のどのサフィックスとも異なる固有のものである限り、当該発行者の選択する如何なる英数字列でもよい。

【００３２】

図６は、ＤＯＩ６００の別の実施例を示しており、図中ではテキストブックのＩＳＢＮ番号がサフィックス６０２として機能している。従って便宜上、元と成るコンテンツの発行者は、サフィックス６０２として元のコンテンツに合致する他のどのような識別コードを選択してもよい。

［強化ＤＯＩ］

図５は更に、強化ＤＯＩ５１０グラマーを図示している。ＤＯＩグラマーを強化する非限定的な実施例は、強化されたプレフィックス５１１として具現される。しかしながら、別の及び／または相補的な強化されたサフィックス（図示はしていない）を同様にＤＯＩ５００に付けてもよいと、全面的に意図されている。強化されたサフィックス５１１は、強化グラマー・ターゲット５１７と強化セパレーター５１４から成る。強化セパレーター５１４は@という記号であるが、当然のことながら、他の文字を強化セパレーターとして指定しても良い。強化グラマー・ターゲット５１７自体は、強化セパレーター５１４以外の任意の文字列である。強化グラマー・ターゲット５１７は、ＤＯＩ５００が特定の情報を多重の種類で解決する目的で用いられ、本開示の中で詳しく述べる。さらに強化された実施例では、強化グラマー・ターゲット５１７自体が更に、強化グラマー動詞５１２と、例えばピリオドのような強化ターゲット・セパレータ５１６によって分離される強化グラマー・ターゲット・オブジェクト５１３から成り得る。もちろん、強化ターゲット・セパレーター５１６は、任意の文字で指定できる。一実施例では、強化グラマー動詞５１２は修飾語として働き、一つのＤＯＩのための複数の多重解決ターゲットの中から選択し、強化

グラマー・ターゲット・オブジェクト５１３は、更なるアクションのために、ターゲット・オブジェクト及び／またはハンドル・システム解決サーバーへと手渡される一つの値である。

［ハンドル・システム・メタデータ］

再び図５を参照すると、ＤＯＩ５００は識別番号に過ぎず、必ずしもそれに関連付けられた情報について何らかの情報を伝達するわけではない。結果として、ＤＯＩにアドレスする情報に関する追加情報を補足して、ユーザーが効率的且つ分かり易いサーチを行い、所望のコンテンツを通信ネットワーク上で入手できるようにすることが望ましい。情報を識別し易くするために、本発明は識別される情報の説明的なデータであるメタデータを使用する。メタデータはＤＯＩに関連するどのようなデータ構造であってもよいが、一実施例によると、メタデータは発行された情報を正確且つ簡潔に識別できる幾つかの基本的なフィールドから成る。この実施例によれば、メタデータは書籍の国際標準図書番号（ＩＳＢＮ）等のレガシー識別スキームからのエンティティと関連する識別子、発行されたコンテンツのタイトル、発行されたコンテンツの種類（書籍、音楽、ビデオ等）、当該コンテンツはオリジナルか派生したものか、コンテンツの主要な著者、コンテンツ作成の際の主要著者の役割、発行者の名前及び／またはその他等から成る。異なる種類のコンテンツはそれを説明する異なるデータを必要とするため、異なる種類のコンテンツには異なるメタデータを使用することを想定しているということがＤＯＩシステムの特徴の一つである。

一実施例によると、メタデータはＤＯＩシステムのユーザー全てに利用可能となっており、それによってユーザーは特定のＤＯＩが識別するエンティティの基本的な説明を検出することが可能である。この基本的な説明によりユーザーはコンテンツを発行したエンティティの、あるいはコンテンツ自体の、幾つかの基本的な事柄を理解することができる。

【００３３】

結果として、ＤＯＩが何の情報を識別するのかを調べるには、それを解決した後、関連するメタデータをレビューすることが望ましい。何故ならばＤＯＩはメタデータを識別するコンテンツや、同じまたは関係するコンテンツに関する別のメタデータとリンクするからである。一実施例では、メタデータによりＤＯＩ５００が識別する情報と共に、その明確な仕様の認識が可能になる。またメタデータにより当該情報とネットワーク上のその他の情報（及びそれらのエンティティに関するメタデータ）とのインタラクションが可能になる。

［ＤＯＩ情報アクセス］

図７と図８は、ＤＯＩハンドル・システムにＤＯＩを提示するだけでユーザーが所望の情報にアクセスできるようにする解決メカニズムの概要を示している。本状況での解決とは、識別子をネットワーク・サービスに提示し、引き換えに当該識別子に関連する最新の情報を一つ以上受け取ることを含む。図７に示すＤＯＩシステムの一実施例では、ユーザー７００はウェブ・ブラウザ・アプリケーションを作動している汎用ワークステーションであり、ＤＯＩ７１０が識別するコンテンツを指し示す。ＤＯＩ７１０は関連するＵＲＬを一つしか持っていないため、そのＵＲＬへと解決されるはずである。その結果、ユーザー７００が特定の識別子７１０が識別する、元と成るコンテンツをリクエストすると、ユーザーは所望のコンテンツがあるＵＲＬ７２０へと導かれる。

従って、このメカニズムにより情報の場所が変更されても、アクション可能な識別子としてエンティティの名前を維持することが可能になる。発行者がコンテンツの場所を変更した場合、発行者はハンドル・システムのデータベース内のＤＯＩエントリーを更新するだけで既存のＤＯＩ７１０は確実にコンテンツの新しい場所を提示する。結果として、コンテンツの場所は変更されてもＤＯＩは変更されず、ユーザーは既存のＤＯＩを用いて新しい場所にある当該コンテンツにアクセスすることが可能である。

【００３４】

図８は、ユーザーがＤＯＩを用いて、同一のＤＯＩが識別した同一のコンテンツの利用可能な複数のコピーの中から、コンテンツへのリクエストと共にコンテンツについてのデータの場所と（例えばコンテンツの購入といった）そのコンテンツに関連するサービスを解

決するＤＯＩシステムの概要を示している。従って、汎用コンピュータであるユーザー８００はウェブ・ブラウザ・アプリケーションを用いて必要なＤＯＩ８３０を提示する。ＤＯＩ８３０は、所望のサービス８３５の種類を説明するように構築することもできる。その結果、ＤＯＩシステムはユーザーがアクセスすることを所望している特定のコンテンツ８４０へと解決することが可能になる。

【００３５】

図９は、本発明に基づき、ユーザーが情報にアクセスするために行う一連のアクションの概要を示している。まず初めに、ユーザーはブラウザ・クライアント９００をパソコン、携帯情報端末（ＰＤＡ）及び／またはその他のコンピューティング・デバイス９０５上に立ち上げる。ユーザーはブラウザ９００を用いてＤＯＩクエリーを作成する。ＤＯＩクエリーは通信ネットワークを通してＤＯＩディレクトリ・サーバー９１０に送られる。ＤＯＩディレクトリ・サーバー９１０のシステムは、ＤＯＩをそこに保存されているエントリーに照らし合わせて調べ、正しいＵＲＬをユーザーのコンピュータ９００上のブラウザ９００に送るが、こうしたアクションはユーザーには見えないようになっている。結果として、ブラウザは正しい発行者情報９２０があるサーバー上の所望のコンテンツへと導かれる。最終的に、ユーザーのブラウザからのリクエストを受け取ると、発行者９２０は所望の情報をユーザーに送り、その情報にはブラウザ・クライアント９００でアクセスすることができる。

図１０は、図９に示すようにユーザーがコンテンツの情報にアクセスするために行う一連のアクションをより詳しく示している。上述したように、ユーザーはブラウザ・クライアント１０００をコンピューティング・デバイス１００５上に立ち上げる。ユーザーはブラウザ１０００を用いてＤＯＩクエリーを作成する。ＤＯＩクエリーは通信ネットワーク上でＤＯＩディレクトリ・サーバー１０１０に送られる。ＤＯＩディレクトリ・サーバー１０１０のシステムは、ＤＯＩをそこに保存されているエントリーに照らし合わせて調べる。ＤＯＩをＤＯＩディレクトリ・サーバー１０１０に保存されているエントリーに照らし合わせて調べた結果、ユーザー１０２５をどこへ導くべきかをＤＯＩディレクトリ・サーバー１０１０は決定する。当該コンテンツの正しいＵＲＬは、何らの中間介入あるいはユーザーによるアクションなしに、自動的にユーザーのブラウザ１０００に送られる。その結果、ブラウザ１０００は元と成るＵＲＬによりアドレスされたサーバーを有する正しい発行者１０２０へと導かれる。当該ＵＲＬは発行者のサーバー１０２０によりユーザーの所望するコンテンツの厳密な場所を決定するために用いられ、発行者のサーバー１０２０は正しいコンテンツ１０３０をユーザーに送る。

図１１は、本発明に基づいて、ＤＯＩを解決して所望のコンテンツが位置するＵＲＬを得ることにより、通信ネットワーク上で情報にアクセスするための幾つかの典型的なメカニズムの概要を示している。一実施例によると、ユーザーは直接ＤＯＩを提示し、ＤＯＩシステムは正しいコンテンツを入手し単に正しいＵＲＬにリンクすることによりそれをユーザーに送信する。別の実施例によると、ユーザーはメタデータに含まれるフィールドの幾つかに関係する情報を提示し、するとＤＯＩルックアップ・サービスは正しいＤＯＩを識別し、それが今度は所望するコンテンツの場所を解決する。図１１に示すように、一実施例によれば、サーチ・エンジン１１０１０をユーザーに提供してもよい。一実施例では、登録機関のＤＯＩとメタデータ・データベースとの通信において、サーチ・エンジンをオファーし配備する。別の実施例では、ｗｗｗ．ｇｏｏｇｌｅ．ｃｏｍのようなサーチ・エンジンを用いて登録機関のデータベースにクエリーを出す。ユーザーは、サーチ・エンジン１１０１０に何らかの識別情報を提示することにより正しいＤＯＩを検索する。サーチ・エンジン１１０１０は提示された識別情報を用いてメタデータに関する自分のデータベースを検索し、提示されたメタデータの情報に関連するＤＯＩを入手する。したがって、サーチを行うユーザーには、メタデータ・データベースから返送したＤＯＩ及び／または前記返送したＯＤＩから解決したＵＲＬを提示し得る。入手したＤＯＩはＤＯＩディレクトリ１１０１１に送られ、ＤＯＩディレクトリ１１０１１は所望のコンテンツを発行者１０４０が置いている場所のＵＲＬを解決する。最終的に、ユーザーのブラウザは正しい

コンテンツ１１０６０へと導かれる。
【００３６】
別の実施例によると、ユーザーはＤＯＩ１１０１５をブラウザ１１０２５のアドレス・ウィンドウ１１０２０に提示する。ユーザーのウェブ・ブラウザが元々ＤＯＩを処理する能力がない場合、ＤＯＩ１１０１５はＤＯＩディレクトリ１１０１１用のプロキシ・サーバーのアドレスを含んでいてもよく、それは図１１においては「ｄｘ．ｄｏｉ．ｏｒｇ」である。その結果、ブラウザはｄｘ．ｄｏｉ．ｏｒｇに位置するＤＯＩディレクトリ１１０１１へと導かれ、ＤＯＩディレクトリ１１０１１は所望のコンテンツを発行者１１０４０が置いている場所のＵＲＬを解決し、ユーザーのブラウザをそこへと導く。
別の実施例によれば、ＤＯＩはドキュメントあるいは何らかの形式の情報１１０３０の中に埋め込むこともでき、それによりＤＯＩをクリックすることによってユーザーを正しいＤＯＩディレクトリ１１０１１に導き、ＤＯＩディレクトリ１１０１１は所望のコンテンツを発行者１１０４０が置いている場所のＵＲＬ決定し、ユーザーのブラウザをそこへと導く。
【００３７】
別の実施例によると、ＤＯＩはＣＤ－ＲＯＭまたはフロッピー・ディスク等のメモリ１１０４０上に提示してもよく、するとメモリは自動的に、または起動されると、ユーザーを正しいＤＯＩディレクトリ１１０１１に導き、ＤＯＩディレクトリ１１０１１は所望のコンテンツを発行者１１０４０が置いている場所のＵＲＬを割り出し、ユーザーのブラウザをそこへと導く。
【００３８】
また別の実施例によれば、ＤＯＩは印刷物としてユーザーに提供してもよく、ユーザーは当該ＤＯＩを上記の如く光学的及び／または機械的周辺入力機器を用いてマニュアルで入力する。
【００３９】
図１２は、通信ネットワーク上で情報を入手し、ＤＯＩシステムがＤＯＩを解決して所望の情報が位置するＵＲＬを得るための典型的なメカニズムの別の実施例の概要を示している。この一実施例によると、複数のＤＯＩディレクトリ１２１０が分散型ＤＯＩディレクトリとして存在し、ハンドル・システム１２００を形成している。一実施例では、分散型ＤＯＩディレクトリはあたかも単一のディレクトリ１１０１１であるかのように動作し、リクエストに応える。その点を除いては解決は図１１と同様に行われる。
図１３は、本発明に基づいた典型的なＤＯＩシステムの概要であり、発行者、ＤＯＩ登録サービス及びハンドル・システムが連携して創り出す効率的なＤＯＩシステムの概要を示している。プレフィックス・ホルダー１３５５は、ＤＯＩ１３４２と関連するメタデータ１３６６から成るＤＯＩ登録サービス１３００に情報を提出する。既に固有のプレフィックス５０１を与えられているプレフィックス・ホルダーは、コンテンツ１３６６にサフィックス５０２を指定するように要求する。登録サービス１３００は、情報１３４２、ハンドル・システム１３５０内に次に預けるための情報１３６６、及び／またはメタデータ・データベース１３１０といったユーザーから提出された情報を解析及び／または再形式設定する役目を担う。上記のように、ＤＯＩを用いてアドレスできるコンテンツの範囲は無限である。その結果、コンテンツ１３６６は如何なる情報及び記事、書籍、音楽アルバムを含む著作物、またはそれらの選択された個別の部分から成ってもよい。ＤＯＩ５００を提供することに加え、発行者１３４２は、コンテンツ１３６６用のメタデータを収集する。当該メタデータは当該コンテンツのＤＯＩ５００、ＤＯＩジャンル、識別子、タイトル、タイプ、起源、主要エージェント、エージェントの役割及び／またはその他から成る。また、様々な相手から提供され識別された、コンテンツに関係のある関連サービスのリストから成っていてもよい。様々な相手とは例えば、コンテンツをオンラインで購入できるウェブ・ページの場所である。
【００４０】
発行者１３４２がコンテンツ１３６６にサフィックス５０２を指定し必要なメタデータを

収集すると、ＤＯＩ５００と当該メタデータはＤＯＩ登録サービス１３００に送信される。ＤＯＩ登録サービス１３００はＤＯＩ５００のデータベース、登録されたコンテンツ１３６６全てのメタデータと共にコンテンツ１３６６が位置するＵＲＬを維持する。本発明によると、ＤＯＩ登録サービス１３００は当該メタデータをメタデータ・データベース１３１０、図１では１１９ｃに送信する。メタデータ・データベース１３１０はＤＯＩ登録サービス１３００が一元管理することもできるし、またそうしなくてもよい。

【００４１】

ＤＯＩ登録サービス１３００は、収集されたメタデータを別のデータ・サービス１３２０に提供したり、付加価値を付けたリソース１３３０をユーザーに提供したりするために利用することもできる。加えて、ＤＯＩ登録サービス１３００は正しいＤＯＩハンドル・データをハンドル・システム１３５０に送り、ハンドル・システムは複数のＤＯＩディレクトリ・サーバー１３４１から成っていてもよい。

［デジタル権利管理］

図１４は従来のデジタル権利管理（ＤＲＭ）シナリオに関わる各者間のインタラクションを図示した機能ブロック図である。従来のＤＲＭシナリオは、発行者１４１０が保護を必要とするデジタル・ワークを作り出すか、手に入れるかすることから始まる。ワーク１４１１はデジタル資産の一例である。発行者１４１０はワーク１４１１をＤＲＭパッケージング・ソフトウェア１４１２に送り、ワーク１４１１と関連付ける権利を特定する。これらの権利は顧客１４５０が行うことができるアクションを規制するもので、顧客がワークを読むこと、ワークを複製すること、ワークを別の顧客に転送すること及びワークを印刷することを含むが、これらに限定されるものではない。これらの権利はまた、時間ベースのものである（例えば、前述のアクションは全て、例えば二週間またはある特定の日から別の日までというような、特定された期間に許可する）。これらの権利はまた特定された回数のイベントに対して許可してもよい（例えば、顧客に二十回だけコンテンツを読むためのアクセスを許可したり、顧客に前もって特定された数の印刷を許可したり、顧客にある人数の受信者にのみコンテンツの転送を許可したり、あるいは顧客に何人の受信者にでも転送することを許可するものの、最初の二十人のリクエスト者にのみアクセスを認めるカウンターを有するセントラル・サーバーからアクセス権利を確保することを全ての受信者に対し要求することにより、最初の二十人の受信者のみにアクセスを許可したりする）。これらの権利はまた様々なセールス・プロモーション、製品またはサービス・バンドリング、あるいはディスカウント及びその他に関連させてもよい。発行者１４１０が指定できるこれらの権利には、数限りないバリエーション、組み合わせ及び順列がある。発行者１４１０はこれらの権利を一つずつ独立に特定してもよい。権利が特定された後、ＤＲＭパッケージング・ソフトウェア１４１２は保護されたワーク１４１３を安全なラッピング及び暗号化１４１４へと転送して、ワークの内容１４１３を暗号化し、ワークを安全なコンテナに入れることができる。ラッピングされた安全なワークは、安全なワーク１４１５として発行者へと戻される。理解されるべきことは、発行者１４１０、ＤＲＭパッケージング・ソフトウェア１４１２、安全なラッピング及び暗号化１４１４は、上記の機能を単一のコンピュータまたは分散型コンピュータ・ネットワークにおいて実行できるということである。更にまた、ＤＲＭパッケージング・ソフトウェア１４１２と安全なラッピング及び暗号化１４１４によって実行される機能は、発行者１４１０に代わって発行者１４１０以外のエンティティにより実行されることもできるということも理解されるべきである。更にまた理解されるべきことは、上記の機能は異なるソフトウェア・モジュールによって、あるいはこれらの様々な機能を組み合わせて一緒にしたりその他の関係する機能や関係の無い機能と組み合わせたりしたソフトウェア・モジュールによって実行されてもよいということである。

【００４２】

発行者１４１０は安全なワーク１４１５をコンテンツ・ホスティング１４２０データベースに保存する。それに加えて、安全なワーク１４１５を説明するデータがメタデータ・データベース１４２２に保存される。理解されるべきことは、発行者１４１０、コンテンツ

・ホスティング１４２０及びメタデータ・データベース１４２２は、上記の機能を単一のコンピュータまたは分散型コンピュータ・ネットワークにおいて実行できるということである。更にまた、ＤＲＭコンテンツ・ホスティング１４２０及びメタデータ１４２２によって実行される機能は、発行者１４１０以外のエンティティにより実行されることもできるということも理解されるべきである。

【００４３】

顧客１４５０は安全なワーク１４１５の複製をデジタル流通という手段を介して得る。顧客１４５０は、発行者１４１０のウェブ・サイトにアクセスして安全なワーク１４１５の複製をダウンロードすることもできる。別の方法として、顧客１４５０がインデックスまたはライブラリ・カタログを閲覧し、発行者１４１０のウェブ・サイトあるいは発行者１４１０以外のエンティティによりホストされているミラー・サイトにある安全なワーク１４１５へのリンクを偶然見つけることもあり得る。あるいは、顧客１４５０は安全なワーク１４１５を別の顧客から直接受信することもでき、つまりそれは「超流通」を介して行われる。上記のように安全なワーク１４１５は発行者１４１０によって安全にラッピングされ暗号化されているので、当該デジタル資産は顧客１４５０にとって無駄なものとなる。

【００４４】

顧客１４５０が安全なワーク１４１５へのアクセスを試みると、権利処理機関１４３０への接続が確立される。権利処理機関１４３０は安全なワーク１４１５に関連するユーザーが誰であるかをチェックし、発行者１４１０が安全なワーク１４１５に関連付けた権利を割り出し、顧客１４５０から安全なワーク１４１５を使用するための代金支払いを受ける。権利処理機関１４３０は電子商取引業者１４３２と関係を築いており、クレジット・カード及びデビット・カードのトランザクションの有効性を確認したり、顧客１４５０に請求書を送ったり、発行者１４１０にトランザクションを報告したりする。電子商取引業者１４３２から肯定的なレスポンスを受信すると、権利処理機関１４３０は顧客１４５０に対し安全なワーク１４１５への鍵または許可証を発行する。顧客１４５０は当該鍵または許可証を用いて保護されたワーク１４１３にアクセスできるようになる。権利処理機関１４３０は、発行者１４１０に総売上額及び個々の顧客情報を報告するためにログまたはデータベースを更新する。理解されるべきことは、発行者１４１０、権利処理機関１４３０及び電子商取引業者１４３２は、上記の機能を単一のコンピュータまたは分散型コンピュータ・ネットワークにおいて実行できるということである。更にまた、権利処理機関１４３０及び電子商取引業者１４３２によって実行される機能は、発行者１４１０以外のエンティティにより実行されることもできるということも理解されるべきである。

【００４５】

別の実施例においては、顧客１４５０はコンテンツ流通業者、シンジゲーターまたは集積業者１４４０を介して安全なワーク１４１５にアクセスすることができる。コンテンツ流通業者、シンジゲーターまたは集積業者１４４０は顧客１４５０がメタデータ・データベース１４２２を閲覧することを許可する。メタデータ・データベース１４２２は、例えばリスティング・サービス、カタログ・サービスまたはセールス・ディレクトリ・サービスを含むが、これらに限定されるわけではない。顧客１４５０が安全なワーク１４１５のようなワークに興味を示すと、コンテンツ流通業者、シンジゲーターまたは集積業者１４４０はコンテンツ・ホスティング１４２０にリクエストを送り、安全なワーク１４１５を入手する。コンテンツ流通業者、シンジゲーターまたは集積業者１４４０はまた権利処理機間１４３０と連結しており、上記のように、安全なワーク１４１５に関連する権利に対する顧客１４５０からの代金支払いをコーディネートする。理解されるべきことは、発行者１４１０、コンテンツ流通業者、シンジゲーターまたは集積業者１４４０は、上記の機能を単一のコンピュータまたは分散型コンピュータ・ネットワークにおいて実行できるということである。更にまた、コンテンツ流通業者、シンジゲーターまたは集積業者１４４０によって実行される機能は、発行者１４１０以外のエンティティにより実行されることもできるということも理解されるべきである。

【００４６】
図１４に図示したシナリオは脆いシステムである。一般的に、オリジナル・デジタル・ワーク１４１１の各インスタンス（即ち保護されたワーク１４１３及び安全なワーク１４１５）は別々のリソースである。更に、オリジナル・デジタル・ワーク１４１１の各インスタンスのコントロールと流通に関わる幾つかのエンティティ（例えば、発行者１４１０、ＤＲＭパッケージング・ソフトウェア１４１２、安全なラッピング及び暗号化１４１４、コンテンツ・ホスティング１４２０及びメタデータ１４２２データベース）があり得る。インターネットをサーチしたり、カタログやピア・ツー・ピア・サーバーを閲覧したりしていて顧客１４５０が見つけるリンクは、古いものであることが多い。同様に、コンテンツ流通業者、シンジゲーターまたは集積業者１４４０も安全なワーク１４１５や保護されたワーク１４１３へのリンクやレファレンスの質を保証することはできない。従って、リンクの脆さを排除しシステムの耐久性を高める装置、方法及びシステムが求められている。

【００４７】
図１４に図示したシナリオは、関係するシステム間に永続的なリンクが無いということだけでなく、別の理由からも脆いシステムである。その理由とは、コンテンツ自体に固有で、明確で、全世界で認識される識別子が無いということである。一般的に、オリジナル・デジタル・ワーク１４１１の各インスタンス（即ち保護されたワーク１４１３及び安全なワーク１４１５）は別々のリソースである。更に、オリジナル・デジタル・ワーク１４１１の各インスタンスのコントロールと流通に関わる幾つかのエンティティ（例えば、発行者１４１０、ＤＲＭパッケージング・ソフトウェア１４１２、安全なラッピング及び暗号化１４１４、コンテンツ・ホスティング１４２０及びメタデータ１４２２データベース）があり得る。仮にこれらのエンティティがコンテンツの固有の識別子に依存できないとすると、これらは簡易性と信頼性を持ってお互いと相互運用すること、つまりコンテンツにレファレンスするための信頼性のある方法を通じてお互いと通信することができない。これは、（バーコードとして知られている）ユニバーサル・プロダクト・コードが必ず信頼性を持って物理的なオブジェクトをレファレンスする数多くのエンティティ間の相互運用性を可能にする方法に似ている。例えば、在庫管理システムと通信しているポイント・オブ・セール（ＰＯＳ）システム、「ジャスト・イン・タイム」補充－注文システムと通信している在庫管理システム、店舗から流通業者または製造元の注文システムに通信している補充－注文システムといったものである。しかしＤＯＩを除けばデジタル・コンテンツのオブジェクトに対しては対応する識別子がなく、よってシステム間通信及び相互運用性を可能にする識別子の欠如に表される脆さをなくすことによりシステムの耐久性を高める装置、方法及びシステムが求められているのである。

【００４８】
図１４はまた、デジタル・オブジェクト識別子（ＤＯＩ）を従来のデジタル権利管理シナリオに組み込むことを図示している。ワークの発行の際に発行者１４１０はそのワークに対し固有のＤＯＩを発行し、それからそれをＤＯＩ登録機関１５５０に登録する。その後ＤＯＩはシステム全体の全てのトランザクションにおいて明確に識別されたワークを指すために用いられる。例えば、コンテンツ・ホスティング・プロバイダー１４２０はＤＯＩに基づいてワークを保存し入手する。この方法ならば、発行者１４１０がコンテンツ・ホスティング・プロバイダーによってホストされているファイル１４１５を更新したい場合は、更新したファイルを同一のＤＯＩにより識別される当該ワークの古いバージョンと置き換えるような指示を付けて送信すればよい。

【００４９】
また別の例では、顧客１４５０にアクセス許可証を販売した権利処理機間１４３０がＤＯＩを用いて発行者の様々なワーク全ての売上額を発行者に継続的ベースで報告する。現在、多くの権利処理機関が発行者に対し売上額の報告を自動化不可能な、マニュアルの方法で、例えばタイトル、著者名及び発行年等の図書目録情報を用いて行い、販売されたワークを明確に識別しようと試みている。これにより発行者１４１０はマニュアルでセールス

の情報を発行者自身のシステムに移さなければならず、また別々に売られたものの殆ど同じ図書目録情報を共有している同一のワークの複数のバージョン間の違いを明らかにする必要があるが、これは保証されていない。各ワークの、そのワークを指す固有のＤＯＩを用いることで全ての当事者が確実に同一のワークを指すようにでき、例えば権利処理機間のセールス・システムと発行者の財務システムといった異なるコンピュータ・システム間の自動相互運用性を可能にする。

【００５０】

信頼性が有り、明確な識別と自動相互運用性の同じ効果は、図１４に図示したＤＲＭシステムのその他の全ての通信チャネルに適用する。例えば、顧客１４５０が保護されたワーク１４１３にアクセスするための鍵を購入すると、当該鍵は正しいもので、同じ著者による別のワークで似通ったタイトルに関連するもの、あるいは異なるフォーマットや言語のもののためのものではないと確信できる。また別の例では、一群の顧客１４５０に対し一人の著者による多数の利用可能なワークを提示したいコンテンツ流通業者、シンジゲーターまたは集積業者１４４０は、メタデータ・データベース１４２２と通信して関係するワークのＤＯＩを調べ、識別されたワークそれぞれのＤＯＩを用いて権利処理リクエストを権利処理機関１４３０に送信し、その後必要に応じて適宜のワークのＤＯＩを用いてコンテンツ・ホスティング・サービス１４２０からワークをダウンロードできる。

［多重解決］

再び第１４図を参照すると、カスタマー１４５０は、ＤＯＩシステムにＤＯＩ解決のリクエストが出されるようにするには、ＤＯＩを直接装置に入力してもよいし、コンテンツ流通業者、シンジゲーターまた集積業者１４４０に頼ってＤＯＩを入力してももよいし、ＤＯＩリクエストを作ることのできるエンド・ユーザーＤＲＭソフトウェアを使用してもよい。ＤＯＩリクエストは、ＤＯＩサーバーに送られ、安全なワーク１４１１に関連するデータに解決するが、これは、しばしばＵＲＬの形をとるポインターである。ＤＯＩは、ＤＯＩシステムになされたリクエストのタイプに応じて、多くのデータの内の一つに解決する。カスタマー１４５０またはコンテンツ流通業者、シンジゲーターまたは集積業者１４４０は、強化ＤＯＩの形をとるＤＯＩリクエストへと解決リクエストのタイプを統合するように選択し得る。一般に、強化ＤＯＩは「ＸＸＸＸ@１０：１０００／ａｂｃ１２３ｄｅｆｇ」の形態をとる。この場合、ＸＸＸＸはＤＯＩシステムへの一つの引数または引数のリストである。発行者１４１０は、引数ＸＸＸＸのためのタイプをＤＯＩサーバーにおいて生成し登録する。例えば、安全にラップされたワークは、ラッパーの中に強化ＤＯＩを含み得る。強化ＤＯＩは、ＧＥＴ．ＲＩＧＨＴＳ@１０．１０００／ａｂｃ１２３ｄｅｆｇといったものであり、権利処理機関の場所に解決する。権利処理機関は代金支払いを受け入れ、許可されたユーザーにコンテンツの鍵を開ける。もし、権利処理機関の場所が移動した場合にか、あるいは発行者が異なる権利処理機関と契約を結んでだ場合には、発行者１４１０がハンドル・システム・ディレクトリ入力を容易に更新でき、全ての既存のＤＯＩに基づいたリンクが、権利処理機関の変更が成される前に生成されたもにもかかわらず、機能し続ける。

更に別の例では、安全化されたコンテンツを受信し、ワークを購入するかどうか決定する前にワークの抜粋にアクセスしたいと希望する顧客がＤＯＩシステムにそのような抜粋のある場所をリクエストすることができる。ＤＯＩシステムは、抜粋を含むページのＵＲＬをもって対応するか、またはユーザーのＤＲＭソフトウェアを安全化されたファイルの僅かな一部分だけを限られた期間において無料で鍵解除できるアクセス鍵へと案内することができる。

［デジタル・ウォーターマーキング］

図１５は図１４に示したデジタル権利管理シナリオにウォーターマークを取り入れることを図示している。発行者１５４４はワーク１５４５に指定する固有のＤＯＩを受け取るためには該ワークをＤＯＩ登録機関１５５０に登録しなければならない。登録機関１５５０はワーク１５４５を説明するメタデータをＤＯＩルックアップ・データベース１５５２に保存する。それに加えて、当該の固有のＤＯＩに関連する数々のサービスが登録され、登

録機関１５５０によってＤＯＩシステム１５３０に登録される。図１５は、発行者１５４４を直接通信接続により登録機関１５５０に連結しているものとして描写している。理解すべきことは、発行者１５４４、登録機関１５５０、ＤＯＩルックアップ・データベース１５５２及びＤＯＩシステム１５３０の間の通信はインターネット１５２０のようなネットワーク上で起こり得るということである。

【００５１】

ワーク１５４５がＤＯＩ登録機関１５５０に登録されると、発行者１５４４はワーク１５４５をウォーターマーキング及びタグ付けシステム１５４２へと転送する。ウォーターマーキング及びタグ付けシステム１５４２は、追加情報がデジタル・ワークの品質を劣化させないような方法で追加情報をデジタル・ワークに加えることにより、ウォーターマークをデジタル・ワーク中に組み込んでいる。デジタル・イメージ、動画またはオーディオ・ファイルにウォーターマークを適用するには数多くの許容可能な従来法が存在するが、本開示ではウォーターマーキングの方法を一つだけ詳細に説明する。ここで開示する新奇な特徴は、デジタル・ウォーターマークに含まれる情報の一部としてのＤＯＩの利用に関する。ＤＯＩは解決可能あるいはアクション可能であるため、ウォーターマークを抽出することができる者なら誰でもＤＯＩを用いてワーク１５４５に関連する所有権の現在の所有者とコンタクトし、当該ワークに関連する様々な登録されたサービスの最新の場所にアクセスすることができる。例えば、あるデジタル・イメージが当該デジタル・イメージのＤＯＩでウォーターマーキングされている場合、ウェブ・サイトで当該デジタル・イメージに遭遇したユーザーはＤＯＩを抽出し自動的に当該デジタル・イメージを再使用する権利のリクエストを出すことができる。ユーザーはまたフォトグラファー及び写真の対象についての最新の情報を入手することもでき、同一の写真の高解像度バージョンを提供してもらい自らの印刷物に使用することもできる。理解すべきことは、発行者１５４４とウォーターマーキング及びタグ付けシステム１５４２は上述の機能を単一のコンピュータまたは分散型コンピュータ・ネットワークにおいて実行できるということである。更にまた、ウォーターマーキング及びタグ付けシステム１５４２によって実行される機能は、発行者１４１０以外のエンティティにより実行されることもできるということも理解されるべきである。

【００５２】

イメージ・ファイルをウォーターマーキングする従来の方法の一つは、最下位ビット・ウォーターマーキングである。標準のイメージ・ファイルはイメージを画像要素つまり画素の格子として表し、各画素はイメージの一領域に対応している。高品質の画像には、画像の各平方インチを表すのに９０，０００画素が必要となる。各画素に、当該画素が対応するイメージの領域を最も良く描写する色と輝度を示す数字が指定される。例えば８ビットのグレー・スケールのイメージでは、各画素に０から２５５の数字を指定してイメージの当該領域の輝度を示し、その場合のバリュー０は黒を表し、バリュー２５５は白を表し、バリュー１２７は中間の濃さのグレーを表す。０から２５５の範囲はベース２つまり二進法で８ビットで表すことができるので、各画素のバリューには８ビットの保存容量が必要となる。例えば、十進法の１５５の画素のバリューをベース２表示に変換したものは「１００１１０１１」（即ち、１００１１０１１（ベース２）＝１＊１２８＋０＊６４＋０＊３２＋１＊１６＋１＊８＋０＊４＋１＊２＋１＊１＝１５５（ベース１０つまり十進法）となる。従って、イメージは二進法の数字の長い数列、つまり０または１にしかならないビットによって表される。

【００５３】

上記の例では、「１００１１０１１」の右端の数字にベースの小さい方の指数をかけるので、右端の数字のバリューがその数字のバリューに最小の影響を与える。従って、右端の数字は「最下位数字」または二進法の数字では「最下位ビット」と呼ばれる。従って十分な深さの（つまり可能なバリューの範囲が十分に広い）イメージ・ファイルの各画素の最下位ビット変更することがイメージの劣化に繋がることは滅多に無い。

【００５４】

最下位ビット・ウォーターマーキングは、選択した画素のバリューの範囲にある各画素バリューの最下位ビットを置き換えることにより、ビットの数列としてのメッセージをイメージ内にエンコードする。このデジタル・ウォーターマーキングの方法は、変更によって変わる各画素のバリューは最高でも１ユニットなので、一般的に人間の目で検知できない。低品質の８ビットのグレー・スケールのイメージでさえも、色の濃度の１ユニットの変更は通常人間の目では検知できない。イメージを観る者が、ウォーターマークを予期し、イメージを分析する方法を知っている場合、ユーザーはエンコードされたメッセージを抽出することができる。

【００５５】

最下位ビット・ウォーターマーキングは「脆いウォーターマーク」として知られている。何故ならば、最下位ビット・ウォーターマーキングは容易に意図的に（即ち、各画素の最下位ビットをゼロに置き換えることによって）または無意識に（つまり、ロスの多いコンプレッサーを用いてイメージを圧縮したり、またはイメージをクロップしたりズームすることにより）ファイルから取り除かれてしまうからである。ウォーターマークをデジタル・ファイル中にエンコードするための、誰でも利用可能な、よりロバストな方法は他にもあり、当該分野で訓練を受けた者にはよく知られている。

【００５６】

図１６Ａは、図１５で示した、結果としてユーザーが保護されたデジタル・ワークを開くことになるウォーター－マーキング・プロセスの一実施例のフロー図である。図１６Ａで示すプロセスは、発行者がデジタル・ワークを作成するステップ１６１０から始まる。ワークが作成されると、ステップ１６１２において発行者は登録機関にコンタクトしてワークに固有のＤＯＩを指定する。ステップ１６１４で、発行者はワークにＤＯＩサービス・バインディングを確立し登録する。最後に、ステップ１６１６で発行者は登録機関にメタデータを登録、保存する。メタデータは、図書目録データ、知覚指紋データ及びチェックサム・データを含むが、これらに限定されるわけではない。ステップ１６１８で、発行者はソフトウェアを用いて、ＤＯＩをウォーターマークとして用いてワークをラッピングし暗号化する。ステップ１６２０で、ユーザーはラッピングされ暗号化されたワークに遭遇し、ＤＯＩに基づくウォーターマークを抽出するＤＲＭソフトウェアを用いてコンテンツを開き、コンテンツへのアクセスを得る。

【００５７】

図１６Ｂは、図１５で示した、結果としてユーザーがハッキングされたデジタル・ワークにアクセスすることになるウォーター－マーキング・プロセスの一実施例のフロー図である。図１６Ｂで示すプロセスは、発行者がデジタル・ワークを作成するステップ１６３０から始まる。ワークが作成されると、ステップ１６３２において発行者は登録機関にコンタクトしてワークに固有のＤＯＩを指定する。ステップ１６３４で、発行者はワークにＤＯＩサービス・バインディングを確立し登録する。最後に、ステップ１６３６で発行者は登録機関にメタデータを登録、保存する。メタデータは、図書目録データ、知覚指紋データ及びチェックサム・データを含むが、これらに限定さるわけではない。ステップ１６３８で、発行者はソフトウェアを用いて、ＤＯＩをウォーターマークとして用いてワークをラッピングし暗号化する。ステップ１６４０で、ユーザーはラッピングされ暗号化されたワークに、当該ワークがハッキングされたりコラプトしてから流通した後に遭遇する。従って、ＤＯＩウォーターマークは有効ではないか、とりだすし不可能である。ステップ１６４４で、再合法化ソフトウェアがハッキングされたりコラプトしたワークを分析し当該ワークの知覚指紋を計算する。ステップ１６４６で、再合法化ソフトウェアがＤＯＩシステムにコンタクトし、メタデータに基づきワークのＤＯＩを探し出し、これによりユーザーはＤＯＩを用いるＤＲＭソフトウェアを用いてコンテンツを開き、コンテンツ及びワークに関連するその他のサービスへのアクセスを得ることができるようになる。

【００５８】

図１６Ｃは、図１５で示した、結果としてユーザーが非公式に流通したデジタル・ワークにアクセスすることになるウォーターマーキング・プロセスの一実施例のフロー図である

。図１６Ｃで示すプロセスは、発行者がワークを含むジャーナルの印刷されたバージョンを流通する等の従来の手段を用いてワークを発行するステップ１６５０から始まる。ワークの従来型の発行に続いて、フローは二つの経路に別れる。一つの経路は誰かがワークのデジタル表現を作成するステップ１６５８から始まり、ステップ１６６０で、非公式の手段を介してデジタル・ワークを流通する。ワークの非公式の流通とは、例えば、ワークのポータブル・データ・フォーマット（ＰＤＦ）バージョンを誰でもアクセスできるウェブサイトにポスティングすることを含む。別の経路は発行者が登録機関にコンタクトしワークに固有のＤＯＩを指定するステップ１６５２から始まる。ステップ１６５４で、発行者はワークにＤＯＩサービス・バインディングを確立し登録する。最後に、ステップ１６５６で発行者は登録機関にメタデータを登録、保存する。ステップ１６６２が、再合法化ソフトウェアを用いてステップ１６５２の固有のＤＯＩをステップ１６６０でワークの非公式に流通したバージョンに付けることによって二つに別れたフローを一つにする。ユーザーはワークの非公式に流通したＰＤＦバージョンをＤＯＩを用いるＤＲＭソフトウェアを用いて開き、コンテンツ及びワークに関連するその他のサービスへのアクセスを得ることができるようになる。

［有効性確認］

図１７は、図１４に示したデジタル権利管理シナリオに有効性確認アーキテクチャを取り入れることを図示している。有効性確認コンピュータ１７３０が保護されたワーク１４１３のようなデジタル・ワークをインターネット１７２０等のネットワークを介して入手する。デジタル・ワークは電子メール・サーバー１７１０、ウェブ・サーバー１７１２または他のユーザー１７１４のコンピュータを含む電子転送ソースから出るものでもよい。代わりに、有効性確認コンピュータ１７３０が取り外し可能なディスク、メモリ保存カードあるいはその他のような物理的な媒体から直接ファイルを読み出すことによりデジタル・ワークを入手してもよい。

【００５９】

有効性確認コンピュータ１７３０上のソフトウェアが入手したばかりのファイルに具現されているワークのＤＯＩを割り出す。これを達成するには様々な方法がある。第一に、ＤＯＩはファイルをダウンロードし有効性確認コンピュータ１７３０のメモリに保存した際にファイルと共に入手することができる。第二に、ＤＯＩはファイルの発行者がファイルに設置したウォーターマークから抽出することもできる。第三に、ワークのＤＯＩはＤＯＩサーチ・エンジン１７４０を使って、周知の図書目録情報（タイトル、著者、発行日等）またはファイルのメタデータ（曲の長さ、イメージ・ファイルまたは曲ファイルの知覚「指紋」、実行可能なファイルのチェックサムまたはハッシュ結果等）を用いたルックアップにより入手することができる。

【００６０】

有効性確認コンピュータ１７３０上のソフトウェアはそれからＤＯＩシステム１７４２にクエリーを発行して、所与のＤＯＩによって識別されたワークのための有効性確認資格認定資料をリクエストする。ＤＯＩシステム１７４２はファイルの資格認定資料もって返答するか、または有効性確認データ収納庫１７４４内のそれらの資格認定資料の場所へのポインター（例えばＵＲＬ）をもって返答する。資格認定資料は周知のタイプのものか、または有効性確認プロセスをどのようにして進めるかについての情報を提供するものでなくてはならない。

【００６１】

有効性確認コンピュータ１７３０上で実行される有効性確認ソフトウェアはそれから、元々入手したファイルの分析を行い、入手した有効性確認資格認定資料と一致するかどうかを判断する。通常、これは元のファイルを入力として用いて一連の計算を行うことに関係し、それらの計算の結果は固定の短い長さとなり、ファイルが最初に発行されてから変更があった場合には異なるものとなる。このようにして、ユーザーはファイルが元々発行されたドキュメントの正当な複製であるかどうか判断できる。ファイルが有効でないか、またはコラプトしたバージョンであると判断された場合は、ソフトウェアは発見したＤＯＩ

を用いて販路を探し出し、ユーザーは直ちにワークの有効な複製を購入あるいは取得する機会を与えられる。

【００６２】

ＭＤ－５やＳＨＡのような、異なる入力に対し同一の出力を生成する可能性の低い、多くの単純なハッシュ・アルゴリズムが存在する。イメージ、音声、動画またはその他のマルチメディア・ファイルの場合は、人間が認知可能なファイル間の差異を検知する有効性確認の方法を用いるのが望ましいかもしれない。そうすれば、曲がユーザーによってＣＤから複製され、別のファイル・フォーマットに変換された場合、それでもアルゴリズムは、認知可能判断基準を用いて、曲が発行されてから変更されたかを判断し、ワークの有効性を確認する。そのような認知アルゴリズムは現在ナップスターがナップスターのファイル共有ネットワーク上でどの曲が取り引きされたかを追跡するために用いられている。ナップスターの認知アルゴリズムについてのより詳細な情報は「ｗｗｗ．ｒｅｌａｔａｂｌｅ．ｃｏｍ／ｎｅｗｓ／ｐｒｅｓｓｒｅｌｅａｓｅｓ／０１０４２０．ｒｅｌｅａｓｅ．ｈｔｍｌ」で見ることができる。

【００６３】

ここに開示した実施例は、デジタル権利管理システムに保護されたデジタル化した著作物にアクセスするための十分に機能する装置、方法及びシステムを描写しているが、読者は他の同等の実施例が存在するということを理解するべきである。本開示を検討する者は数多くの変更やバリエーションを思いつくであろうから、デジタル権利管理システムに保護されたデジタル化した著作物にアクセスするための装置、方法及びシステムは、ここに図示し開示した構成と動作に限定されない。従って、本開示は請求項の範囲を逸脱しない好適な変更全てと同等のもの全てを意図するものとする。

［多重解決メニュー・ファシリティ（ＭＲＭＦ）］

図１８と図１９は、インタラクティブ・インターフェース多重解決メニュー・ファシリティ（ＭＲＭＦ）の一つの非限定的な実施例の概略図である。図１８では、数多くの方法でユーザーにＤＯＩを提供することができる。一例では、ＤＯＩはポータブル・ドキュメント・フォーマット（ＰＤＦ）１８０１に組み込まれ、アドビのアクロバット、アドビのＥブック・リーダー、マイクロソフトのＥブック・リーダー、及び／またはその他のような電子書籍（ｅブック）リーダー１８０５で閲覧される。ＤＯＩ１８０２（例えば図１８では、ＤＯＩはハイライトされたテキスト「ここをクリック」であって、実際にＤＯＩ番号及び／またはレファレンスを、ハイライトされたテキストとしてユーザーに提示されるメタデータとして組み込んでいる）は、ポインティング・カーソル１８０３等のユーザー選択ファシリティにより発動されるが、ユーザー選択ファシリティはこれに限定されるわけではない。ＤＯＩ１８０２を選択することにより、インタラクティブ・インターフェース・メニューが生成される１８０４。ＭＲＭＦは、例えばＣ、Ｃ＋＋、ジャバ、ジャバ・スクリプト、オブジェクティブＣ、パール、パイソン及び／またはその他の数多くの標準開発ツールを用いてモジュールとして実現することができるが、標準開発ツールはそれらに限定されるわけではない。ＭＲＭＦはＤＲＭＳコントローラのユーザー・インターフェースに組み込んでもよい。一つの代替実施例においては、ＭＲＭＦは閲覧アプリケーションのためのプラグ・イン、例えばアドビのアクロバット、アドビのＥブック・リーダー、マイクロソフトのＥブック・リーダー、マイクロソフト・エクスプローラ、マイクロソフト・インターネット・エクスプローラ、ネットスケープ・ナビゲーター及び／またはその他として実現することができるが、プラグ・インはこれらに限定されるものではない。ＭＲＭＦモジュールのロジックは通常、閲覧アプリケーションによって搭載されると発動し、より詳しくはユーザーがＤＯＩ１８０２を選択すると発動する。

【００６４】

カーソル１８０３でＤＯＩ１８０２を発動すると、ＭＲＭＦは、表示し更に選択するための多重解決オプションのリストを得る。当該リストはドキュメントに組み込まれたＤＯＩを読み出しＤＯＩをＤＯＩ解決サーバーで解決することにより生成されるようにしてもよい。一例においては、例えばｐｏｌｌ．ａｌｌＲｅｓｏｌｕｔｉｏｎｓ@ＤＯＩ、ｐｏｌ

ｌ．ａｌｌＡｃｍｅＩｎｃＲｅｓｏｌｕｔｉｏｎｓ@ＤＯＩといった強化ＤＯＩグラマーを用いて、ＤＯＩ解決サーバーからの多重解決オプションを全てをポールすることができる。その後ＤＯＩ解決サーバーは、ＤＯＩ解決サーバーから特定のＤＯＩの記録内に保存されている全ての及び／または幾つかの解決オプションのリストを返信する。ＤＯＩ解決サーバーからこのリストを得ると、ＭＲＭＦは必要に応じて結果を解析し、ＤＯＩ解決サーバー１８０４から返信されてきた解決オプションに対応するメニュー・リストを生成する。

【００６５】

ユーザーに対しオプションのリストを表示すると１８０４、ユーザーは続けてオプションが拡充されたＭＲＭＦ内の表示されたオプションの何れかを選択することができる。それ以降ユーザーは、オプションが拡充されたＭＲＭＦ内に提示され表示された多重解決オプションの一つを、例えばマウスのマウス・ボタンをクリックして、カーソルの選択肢発動メカニズムを発動することによって、選択することができる１８０６、１８０７。注意すべきことは、メニュー・ヒエラルキー１８０４、１８０６、１８０７は、ＤＯＩ解決サーバーのポールの結果を解析することにより構築されるということである。得られた結果は、共通のヘッダーを有する。例えば、ＤＯＩ解決サーバーはポールの結果を、ＢｕｙＢｏｏｋ．Ｐｒｉｎｔ@ＤＯＩ、ＢｕｙＢｏｏｋ．ＡｄｏｂｅＥＢｏｏｋＲｅａｄｅｒ@ＤＯＩ、及びＢｕｙＢｏｏｋ．ＭｉｃｒｏｓｏｆｔＲｅａｄｅｒ@ＤＯＩ、といった強化ＤＯＩの形態で返信し、それらを全て解析して「ＢｕｙＢｏｏｋ」というルートと、「Ｐｒｉｎｔ」、「ＡｄｏｂｅＥＢｏｏｋ」、「ＭｉｃｒｏｓｏｆｔＲｅａｄｅｒ」というサブ・メニューを持つメニューを構築することができる。更に注意すべきことは、ＤＯＩ解決サーバーからのポールの結果それ自体がＤＯＩであってもよく、その場合ＭＲＭＦがかかるポールの結果基づき更に再帰的にポールすることによって、ユーザーのためのより大きな多重解決オプションのメニューを作り上げる。オプションの一つを発動することにより、ＭＲＭＦはユーザーが選択した多重解決オプションへの特定のＤＯＩ解決を開始する。例えば、「ＢｕｙＢｏｏｋ」１８０４、「Ｐｒｉｎｔ」１８０６、「Ａｍａｚｏｎ．ｃｏｍ」１８０７のオプションを選択することにより１８０３、ＭＲＭＦはオプションを、ＤＯＩが表す情報の印刷されたバージョン（及び／またはその他全ての特定されたバージョン）を購入することのできるＡｍａｚｏｎ．ｃｏｍのウェブ・ページへと解決する。

【００６６】

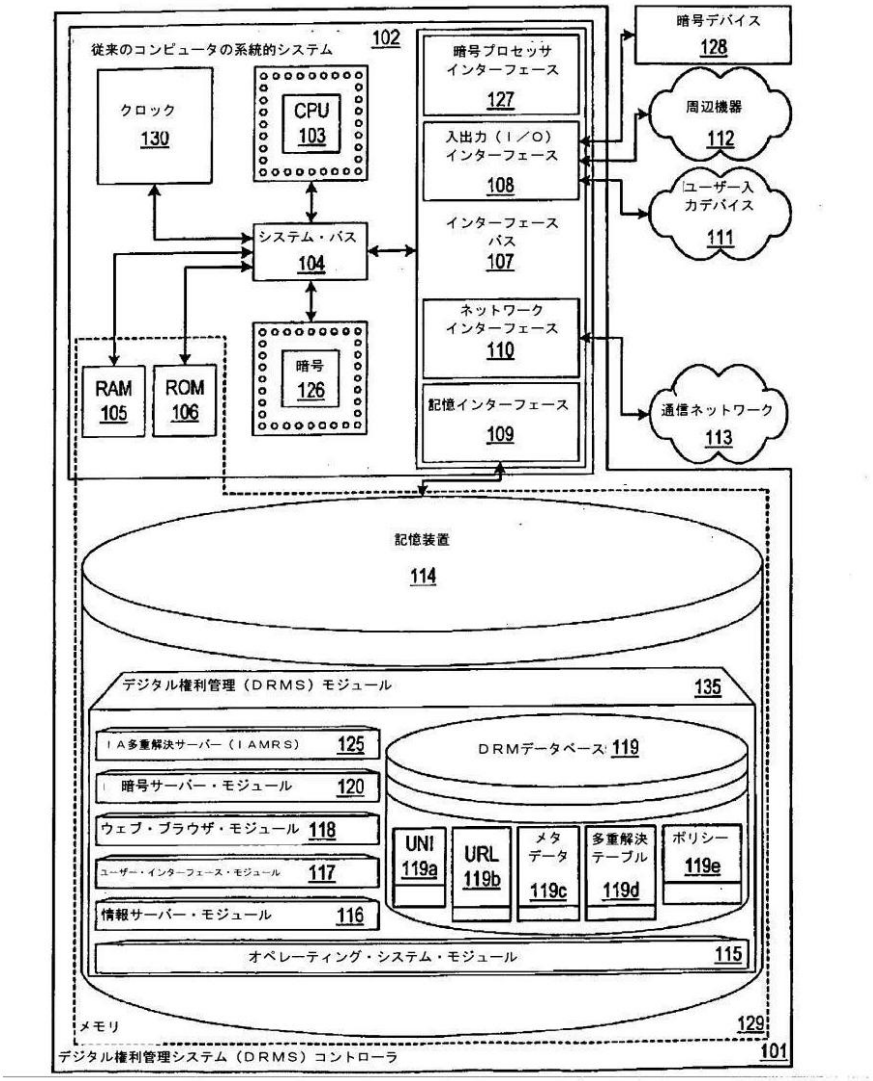
図１９では、一実施例において、ＭＲＭＦは更にユーザーに「Ｅ－ｍａｉｌ　ａ　Ｆｒｉｅｎｄ」のオプション１８０５を提示する。ユーザーが「Ｅ－ｍａｉｌ　ａ　Ｆｒｉｅｎｄ」のオプション１８０５を発動した場合、ＭＲＭＦはオペレーティング・システムに新規の電子メールを生成する信号を生成する。ＭＲＭＦはシステムＡＰＩ、例えばウィン３２ディベロップメント・ライブラリにあるもの、ロータス・ノートＡＰＩ、マイクロソフト・アウトルック・エクスプレスＡＰＩ、マイクロソフト・アウトルック・エクスプレスＡＰＩ及び／またはその他を幾つ用いてでも信号を生成することができる。ＭＲＭＦは適切なＡＰＩを介してコールをして、（必要に応じて電子メール・アプリケーションの立ち上げとインスタンス化と）新規の電子メール・ウィンドウのインスタンス化をリクエストする１９０８。ＭＲＭＦはインスタンス化した電子メール・アプリケーションをそのＡＰＩを介して指示し、ユーザーがそこから選択したＤＯＩ１９０６の複製を持つ新規の電子メールのメッセージを作成する。それ以降、ユーザーはユーザーの友人の電子メール・アドレス１９０７（またはそれ以外の如何なる受信者、例えば配布リスト）に所望のコメント１９０９、１９１０と共に電子メールを宛てて、ＤＯＩを電子メールを介して送り、別のユーザーが当該ＤＯＩとインタラクションできるようにする。

【００６７】

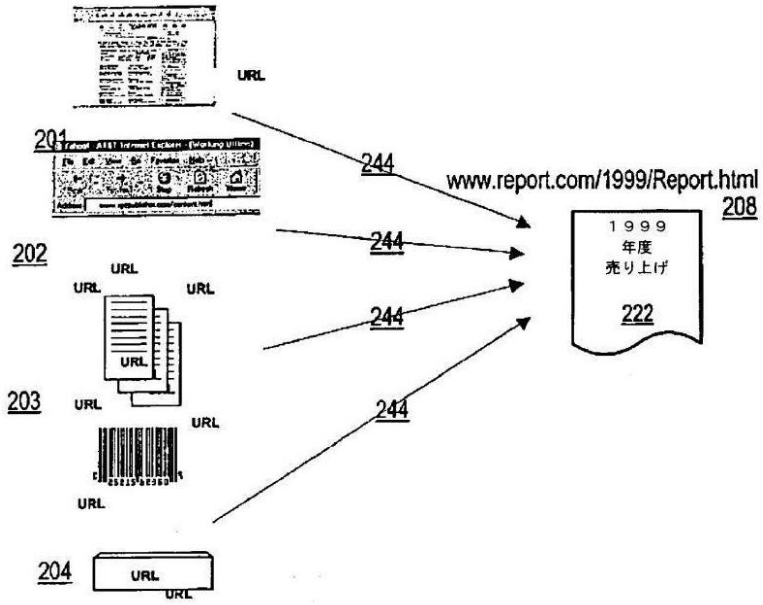
一実施例において、新規の電子メールのメッセージは自動的に生成され、ＭＲＭＦプラグ・インが当該の電子メールのメッセージにプラグ・インをインストールする旨の指示と共に添付され、従ってＭＲＭＦがないところでＭＲＭＦファシリティが可能になるようにしている。別の実施例では、ＤＯＩは、例えばｈｔｔｐ：／／ｗｗｗ．ｄｏｉＲｅｓｏｌｕ

ｔｉｏｎＲｅＲｏｕｔｉｎｇＳｅｒｖｅｒ．ｃｏｍ／ｐｏｌｌ．ａｌｌＲｅｓｏｌｕｔｉｏｎｓ@ＤＯＩというようなハイパーリンクとして組み込まれ、それによって指定されたサーバーがＭＲＭＦ機能を提供できるようにしてある。更に別の実施例では、ＭＲＭＦ機能は、指定されたサーバーから例えばジャバスクリプト、サーバーとの通信に携わるウィンドウ、及び／またはその他等のモジュールをダウンロードすることにより、サーバーによってユーザーのデバイスに提供されている。

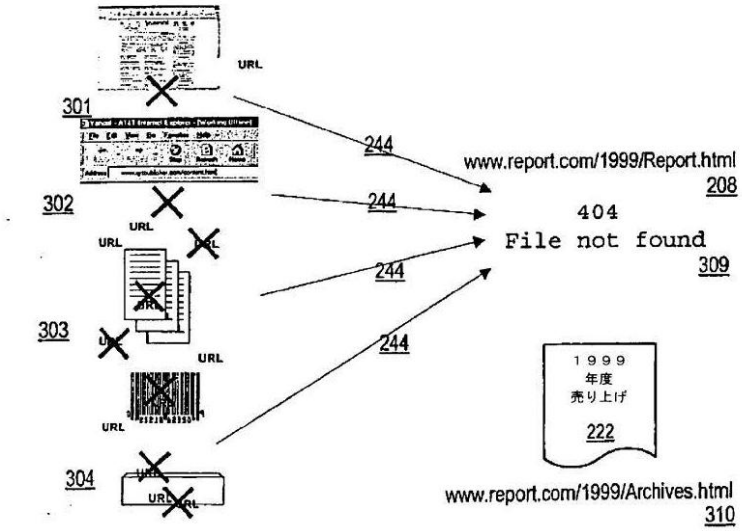
【図１】


従来のコンピュータの系統的システム
102
クロック
130
CPU
103
システム・バス
104
RAM
105
ROM
106
暗号
126
暗号プロセッサ
インターフェース
127
入出力（I／O）
インターフェース
108
インターフェース
バス
107
ネットワーク
インターフェース
110
記憶インターフェース
109
暗号デバイス
128
周辺機器
112
ユーザー入
力デバイス
111
通信ネットワーク
113
記憶装置
114
デジタル権利管理（DRMS）モジュール
135
IA多重解決サーバー（IAMRS）
125
暗号サーバー・モジュール
120
ウェブ・ブラウザ・モジュール
118
ユーザー・インターフェース・モジュール
117
情報サーバー・モジュール
116
DRMデータベース
119
UNI
119a
URL
119b
メタ
データ
119c
多重解決
テーブル
119d
ポリシー
119e
オペレーティング・システム・モジュール
115
メモリ
129
デジタル権利管理システム（DRMS）コントローラ
101

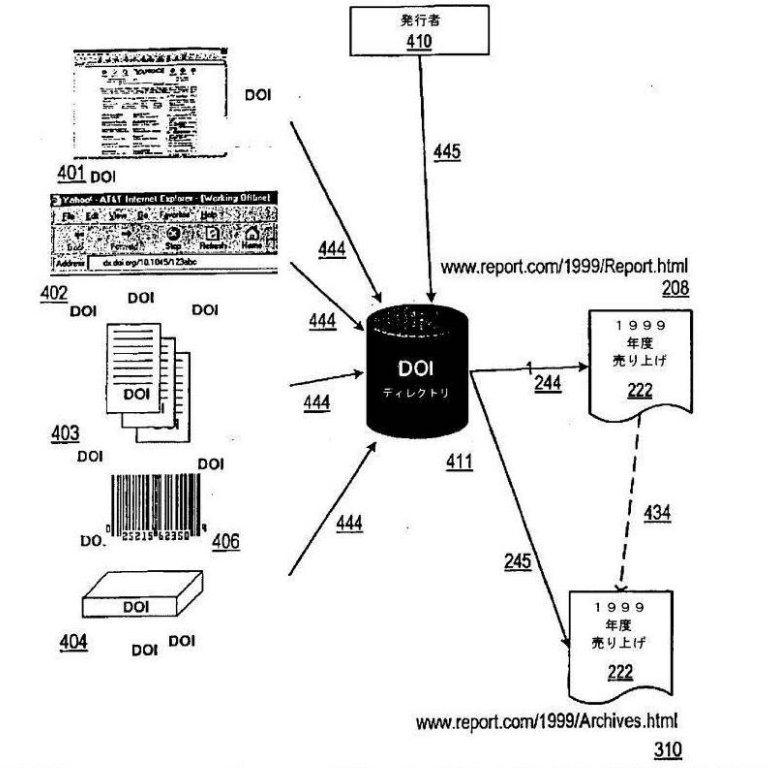
【図２】


URL
201
244
www.report.com/1999/Report.html
208
1999
年度
売り上げ
222
202
URL
URL
URL
URL
244
203
URL
URL
URL
244
URL
204
URL
URL

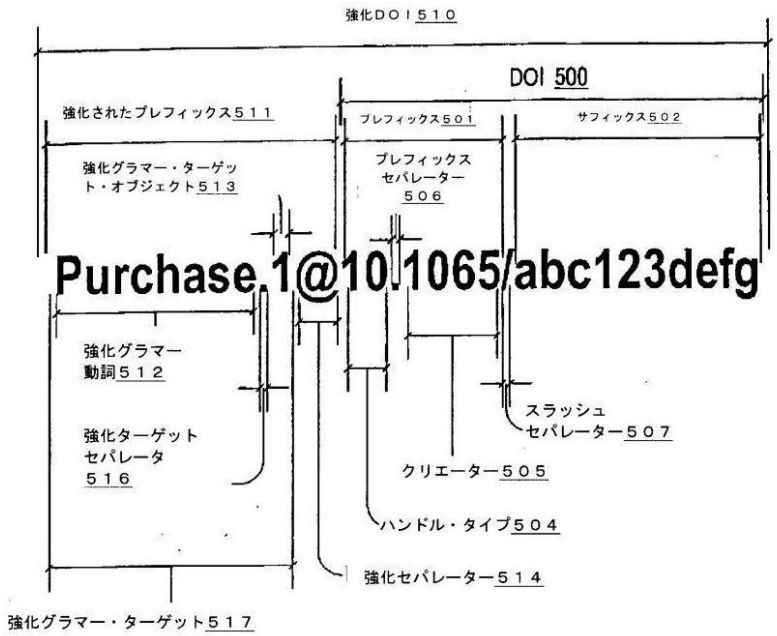
【図３】


URL
301
244
www.report.com/1999/Report.html
208
302
244
404
File not found
309
URL
URL
URL
244
303
URL
URL
244
1999
年度
売り上げ
222
304
URL
URL
URL
www.report.com/1999/Archives.html
310

【図４】


発行者
410
445
DOI
401 DOI
444
www.report.com/1999/Report.html
208
402
DOI
DOI
DOI
444
DOI
ディレクトリ
1999
年度
売り上げ
222
244
DOI
403
DOI
DOI
411
434
444
DO.
406
245
DOI
404
DOI
DOI
1999
年度
売り上げ
222
www.report.com/1999/Archives.html
310

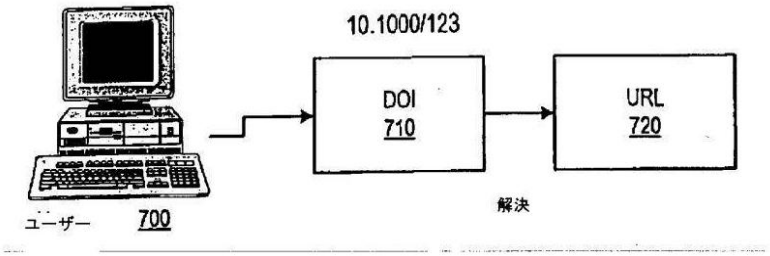
【図５】


強化DOI 510
DOI 500
強化されたプレフィックス511
プレフィックス501
サフィックス502
強化グラマー・ターゲット・オブジェクト513
プレフィックス
セパレーター
506
Purchase.1@10.1065/abc123defg
強化グラマー
動詞512
強化ターゲット
セパレータ
516
スラッシュ
セパレーター507
クリエーター505
ハンドル・タイプ504
強化セパレーター514
強化グラマー・ターゲット517

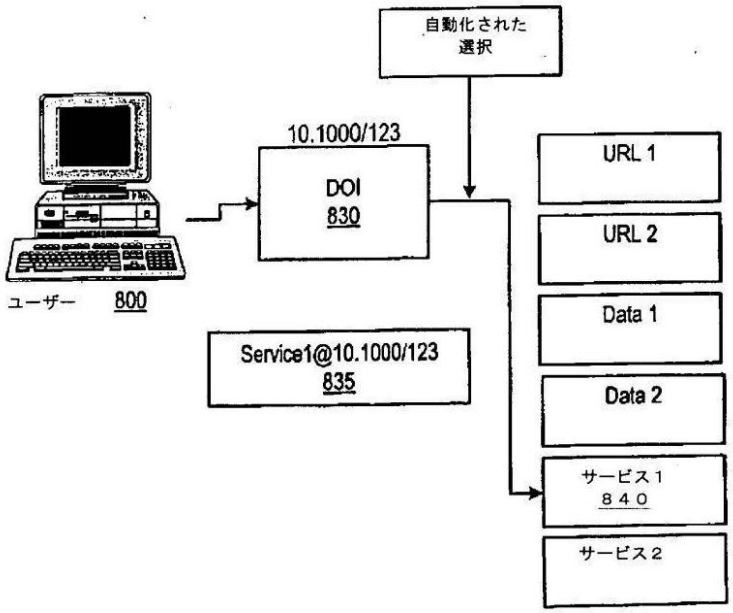
【図６】


プレフィックス501
サフィックス602
10.1065/ISBN-900512-44-9
600

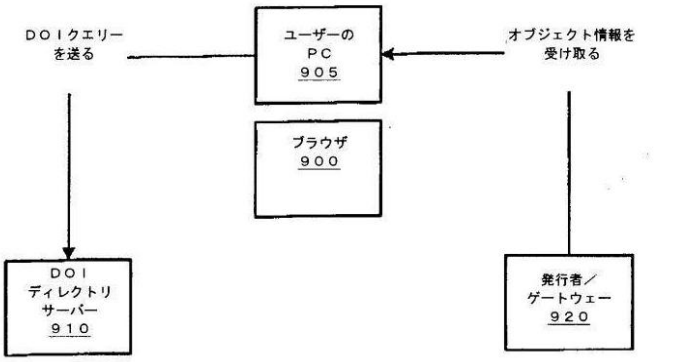
【図７】


10.1000/123
DOI
710
URL
720
解決
ユーザー
700

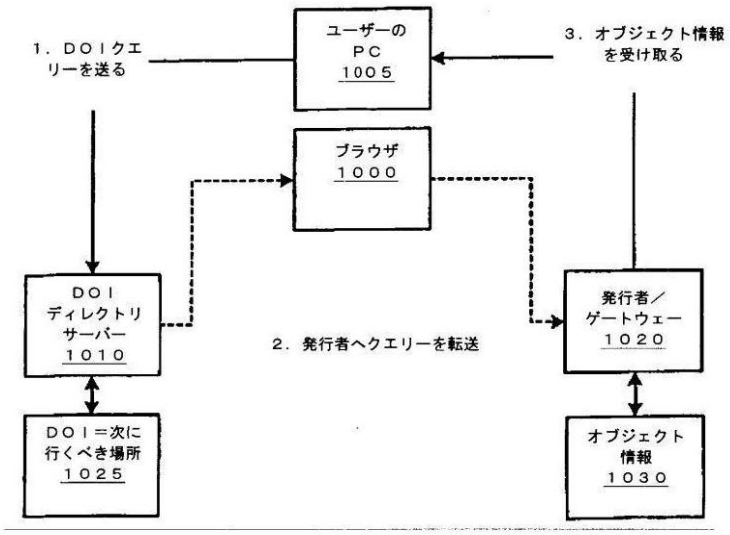
【図８】


自動化された
選択
10.1000/123
DOI
830
URL 1
URL 2
Data 1
Data 2
サービス１
８４０
サービス２
Service1@10.1000/123
835
ユーザー
800

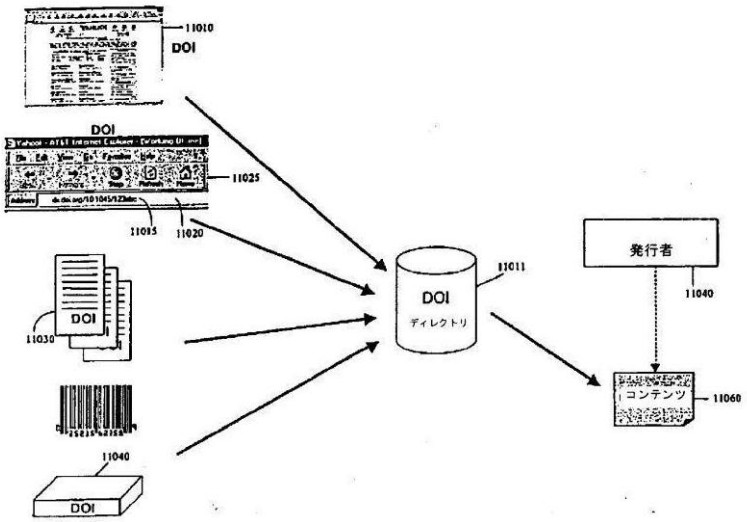
【図９】


ＤＯＩクエリー
を送る
ユーザーの
ＰＣ
９０５
オブジェクト情報を
受け取る
ブラウザ
９００
ＤＯＩ
ディレクトリ
サーバー
９１０
発行者／
ゲートウェー
９２０

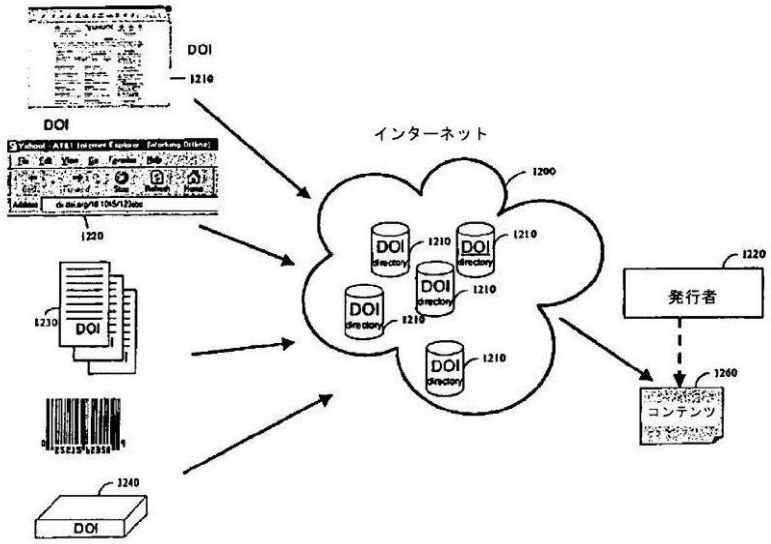
【図１０】


１．ＤＯＩクエ
リーを送る
ユーザーの
ＰＣ
１００５
３．オブジェクト情報
を受け取る
ブラウザ
１０００
ＤＯＩ
ディレクトリ
サーバー
１０１０
２．発行者へクエリーを転送
発行者／
ゲートウェー
１０２０
ＤＯＩ＝次に
行くべき場所
１０２５
オブジェクト
情報
１０３０

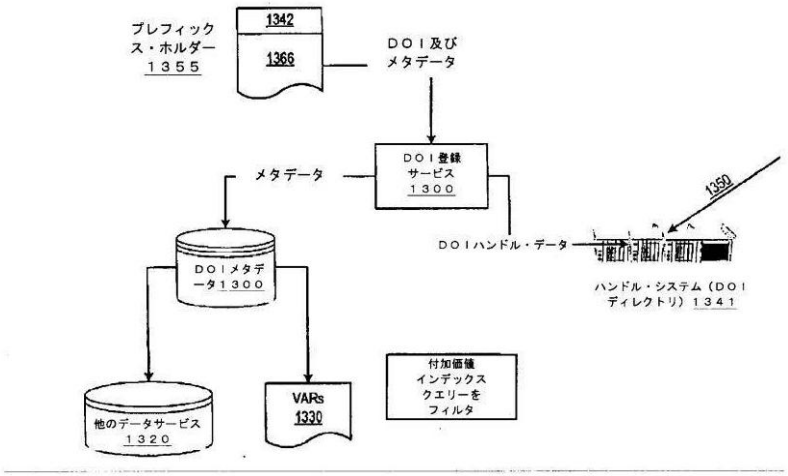
【図１１】


11010
DOI
DOI
11025
11015
11020
DOI
11030
11040
DOI
DOI
ディレクトリ
11011
発行者
11040
コンテンツ
11060

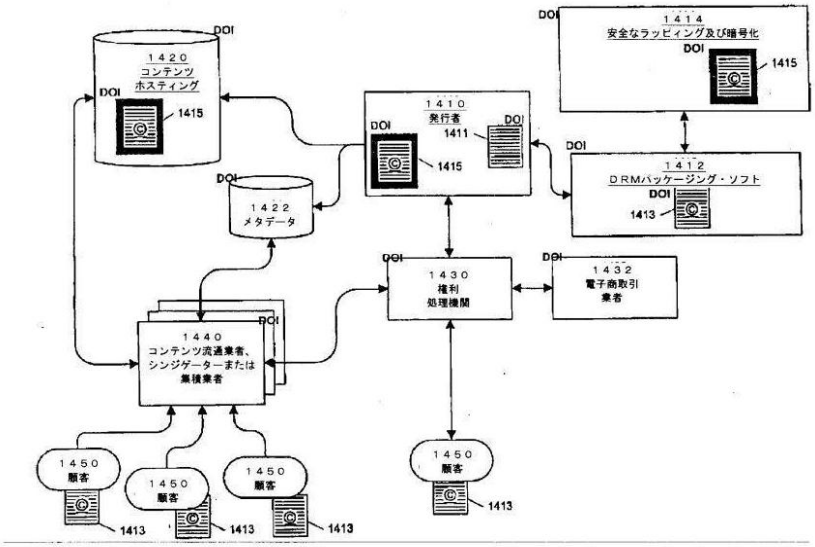
【図１２】


DOI
1210
DOI
1220
インターネット
1200
DOI
directory
1210
1230
DOI
1240
DOI
発行者
1220
1260
コンテンツ

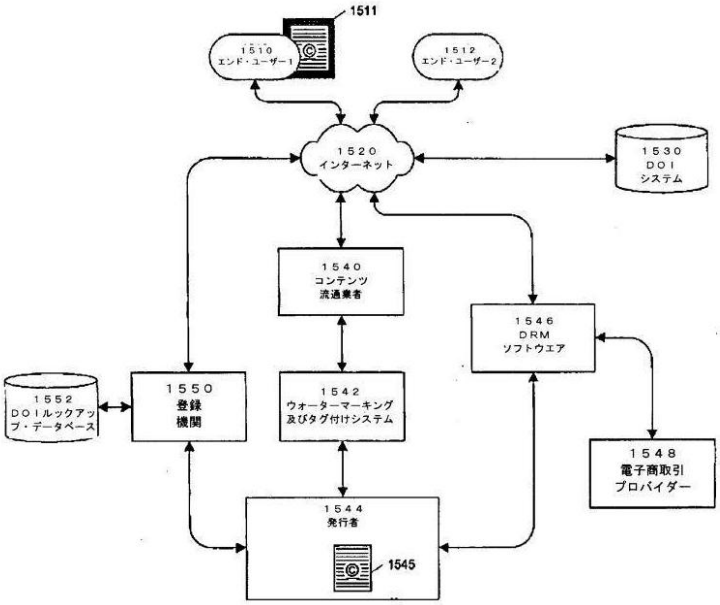
【図１３】


プレフィックス・ホルダー
１３５５
1342
1366
ＤＯＩ及びメタデータ
ＤＯＩ登録サービス
１３００
メタデータ
1350
ＤＯＩハンドル・データ
ＤＯＩメタデータ１３００
ハンドル・システム（ＤＯＩディレクトリ）１３４１
付加価値インデックスクエリーをフィルタ
他のデータサービス
１３２０
VARs
1330

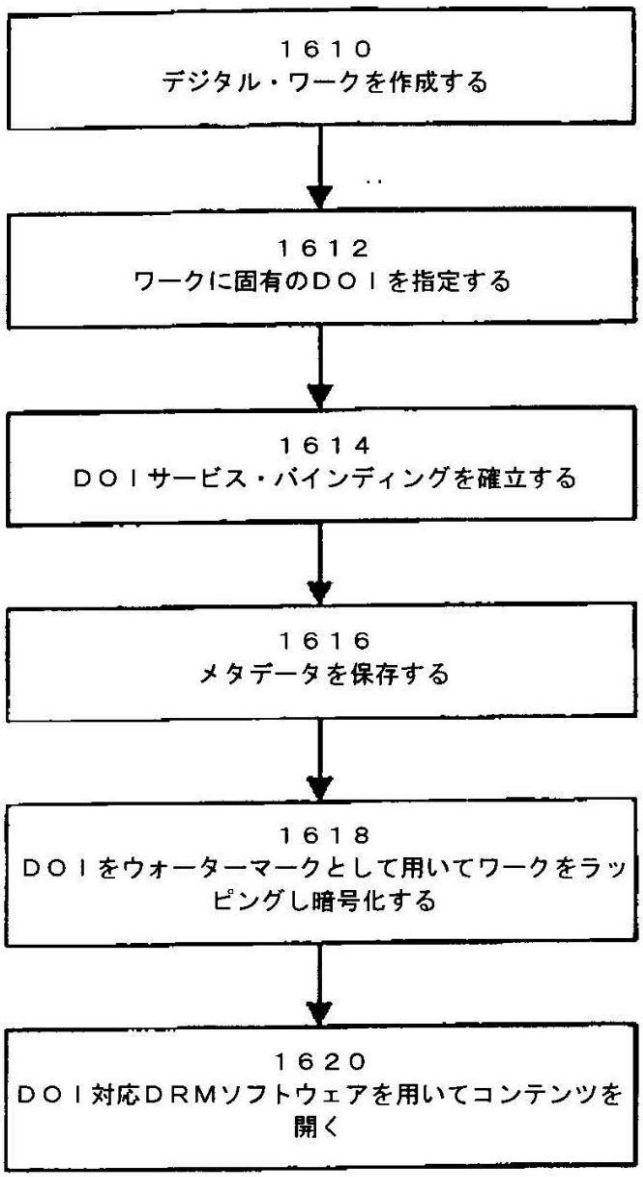
【図１４】


DOI
１４２０
コンテンツホスティング
1415
１４１４
安全なラッピング及び暗号化
１４１０
発行者
1411
１４１２
ＤＲＭパッケージング・ソフト
1413
１４２２
メタデータ
１４３０
権利処理機関
１４３２
電子商取引業者
１４４０
コンテンツ流通業者、シンジケーターまたは集積業者
１４５０
顧客

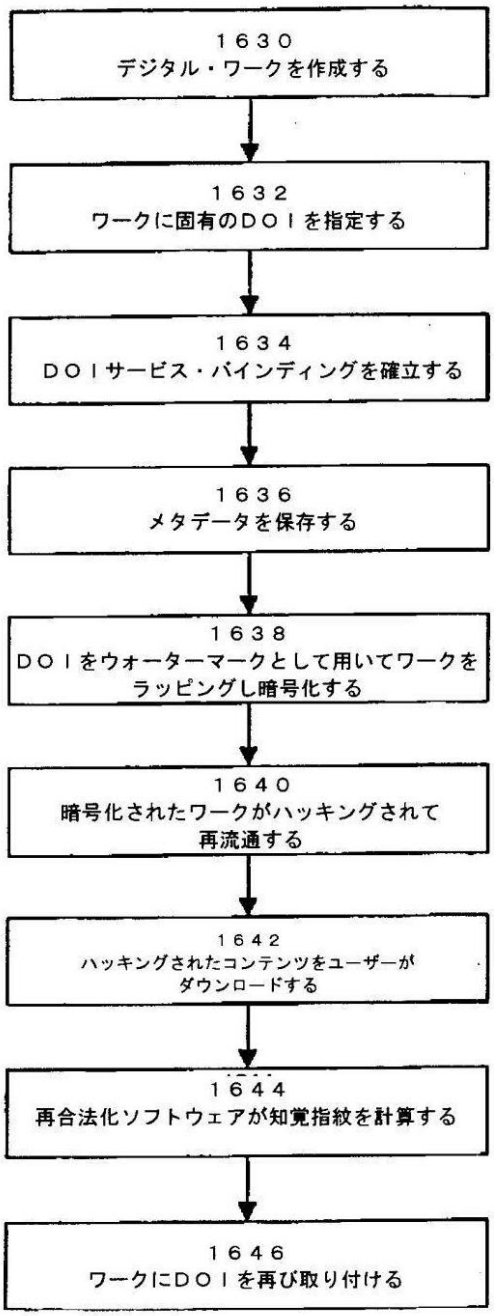
【図１５】


1511
1510
エンド・ユーザー1
1512
エンド・ユーザー2
1520
インターネット
1530
DOI
システム
1540
コンテンツ
流通業者
1546
DRM
ソフトウエア
1552
DOIルックアップ・データベース
1550
登録
機関
1542
ウォーターマーキング
及びタグ付けシステム
1548
電子商取引
プロバイダー
1544
発行者
1545

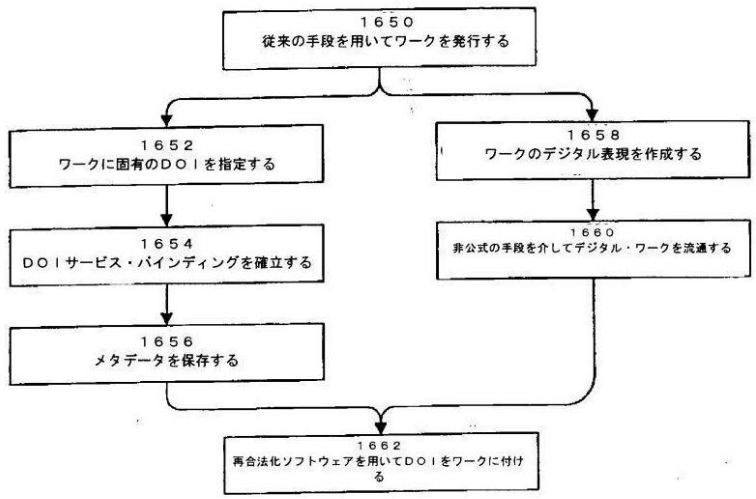
【図１６Ａ】


１６１０
デジタル・ワークを作成する
１６１２
ワークに固有のＤＯＩを指定する
１６１４
ＤＯＩサービス・バインディングを確立する
１６１６
メタデータを保存する
１６１８
ＤＯＩをウォーターマークとして用いてワークをラッピングし暗号化する
１６２０
ＤＯＩ対応ＤＲＭソフトウェアを用いてコンテンツを開く

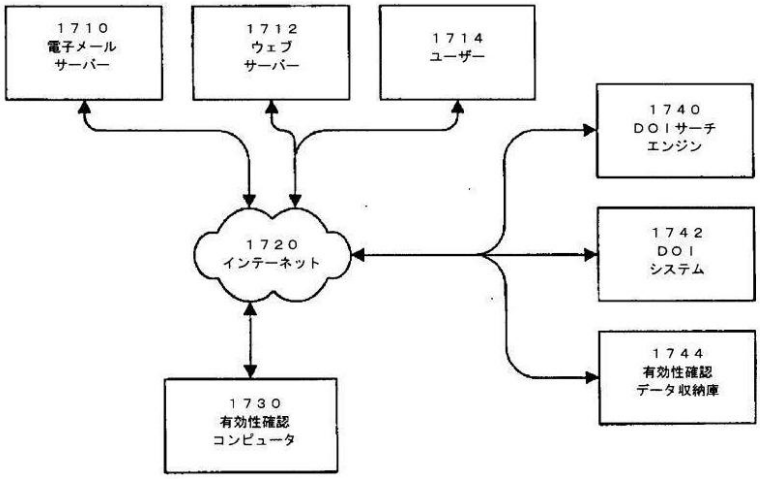
【図１６Ｂ】


１６３０
デジタル・ワークを作成する
１６３２
ワークに固有のＤＯＩを指定する
１６３４
ＤＯＩサービス・バインディングを確立する
１６３６
メタデータを保存する
１６３８
ＤＯＩをウォーターマークとして用いてワークを
ラッピングし暗号化する
１６４０
暗号化されたワークがハッキングされて
再流通する
１６４２
ハッキングされたコンテンツをユーザーが
ダウンロードする
１６４４
再合法化ソフトウェアが知覚指紋を計算する
１６４６
ワークにＤＯＩを再び取り付ける

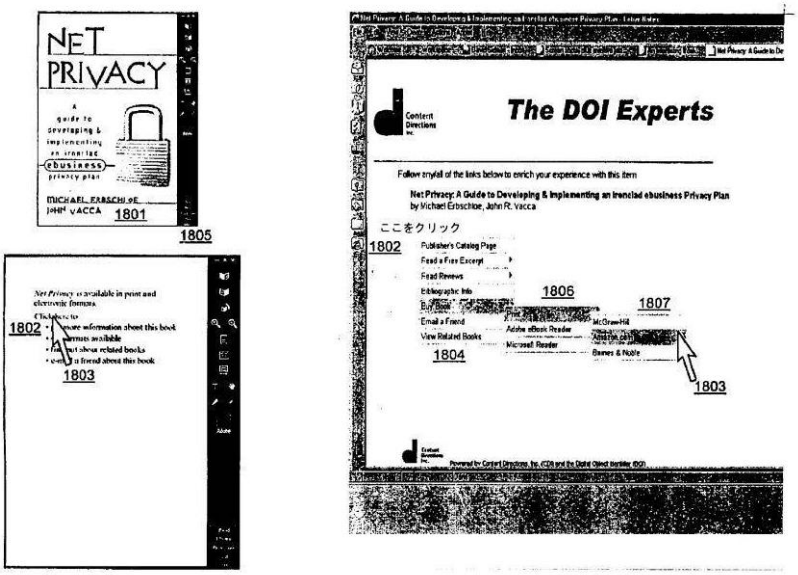
【図１６Ｃ】


１６５０
従来の手段を用いてワークを発行する
１６５２
ワークに固有のＤＯＩを指定する
１６５８
ワークのデジタル表現を作成する
１６５４
ＤＯＩサービス・バインディングを確立する
１６６０
非公式の手段を介してデジタル・ワークを流通する
１６５６
メタデータを保存する
１６６２
再合法化ソフトウェアを用いてＤＯＩをワークに付ける

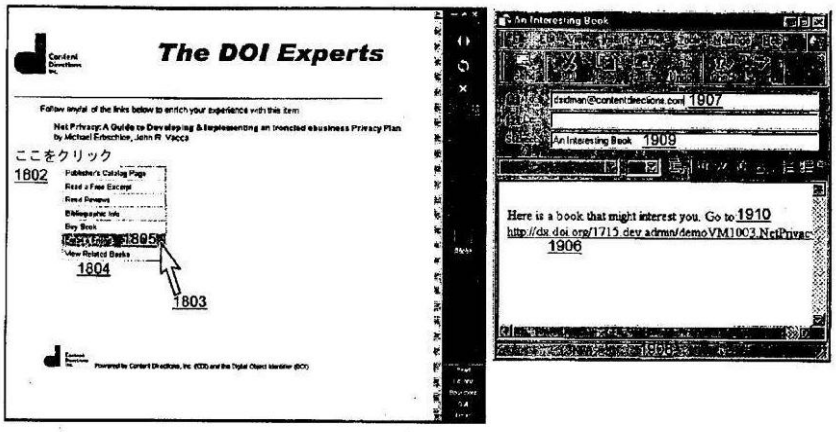
【図１７】


１７１０
電子メール
サーバー
１７１２
ウェブ
サーバー
１７１４
ユーザー
１７４０
ＤＯＩサーチ
エンジン
１７２０
インテーネット
１７４２
ＤＯＩ
システム
１７４４
有効性確認
データ収納庫
１７３０
有効性確認
コンピュータ

【図１８】


NET PRIVACY
1801
1805
1802
1803
The DOI Experts
ここをクリック
1802
1806
1807
1804
1803

【図１９】


The DOI Experts
ここをクリック
1802
1804
1803
An Interesting Book
1907
1909
Here is a book that might interest you. Go to 1910
1906

【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 August 2002 (01.08.2002)

PCT

(10) International Publication Number
WO 02/060110 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/US02/02322

(22) International Filing Date: 25 January 2002 (25.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/264,333	25 January 2001 (25.01.2001)	US
60/267,875	8 February 2001 (08.02.2001)	US
60/267,899	9 February 2001 (09.02.2001)	US
60/268,766	14 February 2001 (14.02.2001)	US
60/270,473	21 February 2001 (21.02.2001)	US
60/276,459	16 March 2001 (16.03.2001)	US
60/279,792	29 March 2001 (29.03.2001)	US
60/303,768	10 July 2001 (10.07.2001)	US
60/328,275	9 October 2001 (09.10.2001)	US
60/328,274	9 October 2001 (09.10.2001)	US
60/328,270	9 October 2001 (09.10.2001)	US

(71) Applicant and
(72) Inventor: SIDMAN, David [US/US]; 558 9th Street, Brooklyn, NY 11215 (US).

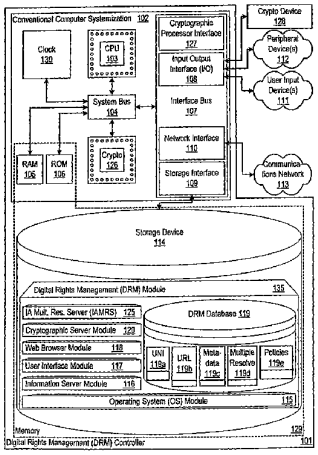
(74) Agent: HANCHUK, Walter, G.; Morgan & Finnegan, L.L.P., 345 Park Avenue, New York, NY 10154 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: APPARATUS, METHOD, AND SYSTEM FOR ACCESSING DIGITAL RIGHTS MANAGEMENT INFORMATION



(57) Abstract: Digital rights management (DRM) and content distribution systems need to reference unique works of autorship to facilitate distribution, access control, and usage tracking and reporting of the works. The apparatus, method, and system disclosed herein is a DRM and content distribution system that uses the digital object identifier (DOI) as a unique identifier for the works of authorship that are the subject of transactions within the system and that travel with the instantiations of the works of authorship. A method of accessing a digital work from a computer is disclosed. The method associates at least one usage right with the digital work to create a protected digital work. The usage rights include displaying the digital work, copying the digital work, fowarding the digital work to another computer, or printing the digital work. The method selects a unique identifier such as a DOI for the digital work and stores the protected digital work and the unique identifier in a directory such as a library of digital works of autorship or a portion of a peer-to-peer network. The method issues a query from the computer to the directory to generate a result set that includes the unique identifier. The method uses the unique identifier to retrieve the protected digital work from the directory. Furthermore, a method is taught to employ multiple resolution capabilities for the super-distribution of DOI referenced content via E-mail and otherwise.

WO 02/060110 A2

WO 02/060110 A2

European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

without international search report and to be republished upon receipt of that report

APPARATUS, METHOD, AND SYSTEM FOR ACCESSING DIGITAL RIGHTS MANAGEMENT INFORMATION

RELATED APPLICATIONS

The instant application hereby claims priority to the following US provisional patent applications: (1) serial number 60/264,333 for "Reference Linking with DOIs" filed on January 25, 2001 (attorney docket number 4188-4001); (2) serial number 60/268,766 for "Apparatus, Method, and System for Multiple Resolution Affecting Information Access" filed on February 14, 2001 (attorney docket number 4188-4002); (3) serial number 60/276,459 for "Apparatus, Method, and System for Registration Effecting Information Access" filed on March 16, 2001 (attorney docket number 4188-4003); (4) serial number 60/279,792 for "Apparatus, Method and System For Directory Quality Assurance" filed on March 29, 2001 (attorney docket number 4188-4004); (5) serial number 60/303,768 for "Apparatus, Method, and System for Accessing Digital Rights Management Information" filed on July 10, 2001 (attorney docket number 4188-4005); (6) serial number 60/328,275 for "Apparatus, Method and System For Accessing Digital Rights Management Information" filed on October 9, 2001 (attorney docket number 4188-4005US1); (7) serial number 60/267,875 for "Apparatus, Method, and System for Accessing Information" filed on February 8, 2001 (attorney docket number 4188-4006); (8) serial number 60/267,899 for "Provisional filing for Apparatus, Method, and System for Accessing Information" filed on February 9, 2001 (attorney docket number 4188-4007); (9) serial number 60/270,473 for "Business Value and Implementation Considerations For The DOI" filed on February 21, 2001 (attorney docket number 4188-4008); (10) serial number 60/328,274 for "Apparatus, Method And System For Effecting

Information Access In A Peer Environment" filed on October 9, 2001 (attorney docket number 4188-4010); (11) serial number 60/328,270 for "Apparatus, Method and System For Tracking Information Access" filed on October 9, 2001 (attorney docket number 4188-4011); each of these applications being herein incorporated by reference.

The instant application, also, hereby incorporates by reference the following Patent Cooperation Treaty applications: (12) for an "Apparatus, Method and System For Multiple Resolution Affecting Information Access" (attorney docket number 4188-4002PC), which was filed on January 25, 2002 in the name of David Sidman; (13) for an "Apparatus, Method and System For Registration Effecting Information Access" (attorney docket number 4188-4003PC), which was filed on January 25, 2002 in the name of David Sidman; (14) for an "Apparatus, Method and System For Directory Quality Assurance" (attorney docket number 4188-4004PC), which was filed on January 25, 2002 in the name of David Sidman; (15) for an "Apparatus, Method and System For Effecting Information Access in a Peer Environment," (attorney docket number 4188-4010PC), which was filed on January 25, 2002 in the name of David Sidman; and (16) for an "Apparatus, Method and System For Tracking Information Access," (attorney docket number 4188-4011PC), which was filed on January 25, 2002 in the name of David Sidman.

FIELD

An apparatus, method, and system for accessing a digitized work of authorship protected by a digital rights management system is disclosed. In particular, the apparatus, method, and system integrates digital object identifiers into the digital rights management system to make the system more durable and provide multiple resolution, reporting,

watermarking, and validation capabilities.

BACKGROUND OF THE INVENTION

Internet

As Internet usage increases, the amount of information available on the Internet also increases. The information that exists on the Internet is of many different types, including documents in many formats such as: computer software, databases, discussion lists, electronic journals, library catalogues, online information services, mailing lists, news groups, streaming media, and the like. Fortunately, much of the information on the Internet can be accessed through the World-Wide-Web using a web browser to interact with the network in a user-friendly way.

Networks

Networks are commonly thought to consist of the interconnection and interoperation of clients, servers, and intermediary nodes in a graph topology. It should be noted that the term "server" as used herein refers generally to a computer, other device, software, or combination thereof that processes and responds to the requests of remote users across a communications network. Servers serve their information to requesting "clients." A computer, other device, software, or combination thereof that facilitates, processes information and requests, and/or furthers the passage of information from a source user to a destination user is commonly referred to as a "node." Networks are generally thought to facilitate the transfer of information from source points to destinations.

Transmission Control Protocol / Internet Protocol (TCP/IP)

The proliferation and expansion of computer systems, databases, and networks of computers has been facilitated by an interconnection of such systems and networks in an

extraterritorial communications network commonly referred to as the Internet. The Internet has developed and largely employs the Transmission Control Protocol-Internet Protocol (TCP/IP). TCP/IP was developed by a Department of Defense (DoD) research project to interconnect networks made by various and varying network vendors as a foundation for a network of networks, i.e., the Internet. The development of TCP/IP was in part driven by a requirement by the DoD to have a network that will continue to operate even if damaged during battle, thus allowing for information to be routed around damaged portions of the communications network to destination addresses. Of course, if the source or destination address location itself is rendered inoperable, such delivery will not be possible.

The Internet is a packet-switched network and thus, information on the Internet is broken up into pieces, called packets, and transmitted in packet form. The packets contain IP addressing information called headers, which are used by routers to facilitate the delivery of the packets from a source to a destination across intermediary nodes on the Internet. Upon arrival at the destination, the packets are reassembled to form the original message, and any missing packets are requested again.

The IP component of the protocol is responsible for routing packets of information based on a four byte addressing mechanism; the address is written as four numbers separated by dots, each number ranging from 0 to 25 5, e.g., "123.255.0.123". IP addresses are assigned by Internet authorities and registration agencies, and are unique.

The TCP portion of the protocol is used for verifying that packets of information are correctly received by the destination computer from the source, and if not, to retransmit corrupt packets. Other transmission control protocols are also commonly used that do not guarantee delivery, such as User Datagram Protocol (UDP).

World-Wide-Web

The proliferation and expansion of the Internet, and particularly the World-Wide-Web (the web), have resulted in a vast and diverse collection of information. Various user interfaces that facilitate the interaction of users with information technology systems (i.e., people using computers) are currently in use. An information navigation interface called WorldWideWeb.app (the web) was developed in late 1990. Subsequently, information navigation interfaces such as web browsers have become widely available on almost every computer operating system platform.

Generally, the web is the manifestation and result of a synergetic interoperation between user interfaces (e.g., web browsers), servers, distributed information, protocols, and specifications. Web browsers were designed to facilitate navigation and access to information, while information servers were designed to facilitate provision of information. Typically, web browsers and information servers are disposed in communication with one another through a communications network. Information Servers function to serve information to users that typically access the information by way of web browsers. As such, information servers typically provide information to users employing web browsers for navigating and accessing information on the web. Microsoft's Internet Explorer and Netscape Navigator are examples of web browsers. In addition, navigation user interface devices such as WebTV have also been implemented to facilitate web navigation. Microsoft's Information Server and Apache are examples of information servers.

Universal Resource Locator (URL)

The expansion of the web has resulted in an enormous quantity of information, which is accessible through the use of Universal Resource Locators (URLs). An URL is an address

that is typically embodied as a hyperlink in a web page or is typed into a web browser. URLs for a given resource (most commonly a file located on a remote computer) refer only to a location for that resource. Typically, the reference to the location is achieved through the use of an unresolved IP address in conjunction with a directory path and file name; e.g., "http://www.aWebSite.com/aFolder/aFile.html". In this example, the URL directs the browser to connect to the computer named "www" in the domain "aWebSite.com," and to request the file named "aFile.html" stored in directory "aFolder" at that computer.

Universal Name Identifier (UNI)

The Corporation for National Research Initiatives has created and implemented a new means of naming and locating information, called the Handle System. The Handle System is designed to improve upon the current use of URLs.

The Handle System introduces a level of indirection to locating and distributing information over the Internet. The Handle System is a general-purpose system for naming resources. Instead of being assigned a URL based on a particular resource's current network location, a resource may be assigned a Universal Name Identifier. A UNI is a form of Universal Resource Identifier (URI). URIs include both UNIs and URLs. A UNI, unlike a URL, serves and shall be regarded henceforth as a name for the resource that is persistent regardless of changes in the resource's location or other attributes. In turn, a Universal Resource Name (URN) is a type of UNI (i.e., a UNI subsumes the concept of a URN). Furthermore, a Handle is a type of URN. And a Digital Object Identifier (DOI) is a type of Handle. Thus, various forms of UNIs include Handles, URNs, DOIs, and/or the like. The various terms and/or forms of UNIs will be used interchangeably throughout this document, and may be assumed to be interchangeable unless stated otherwise. A Handle is a unique

name that is registered with the Handle System along with the current network location of the named resource and the location of relevant associated services. This location information commonly takes the form of a URL. One common type of Handle is known as a Digital Object Identifier (DOI). Handles may be then distributed to users in lieu of a URL, and superficially appear to function similarly to a hyperlink. When a user encounters a Handle, the user may select or enter the Handle much like a URL hyperlink, so long as the user's web browser is capable of making Handle requests. Such an encounter triggers an automated process to look up a resource's current location. The current location of the resource is associated with the resource's Handle in a directory made available by the Handle System, which in turn directs the user to the resource's current location. The same process can be invoked to redirect users to services associated with an identified work. Unlike with a URL, if the resource or service moves, the Handle System directory entry can be updated, thereby assuring a persistent association between a Handle and the resources or services it identifies. Knowing only a URL for a given resource is akin, in the physical world, to knowing only a person's street address, and not her name. If she were to move across town, it would be very difficult to locate her without knowing her name. The Handle System allows resources to be permanently named by way of a Handle, and it allows the current network location of resources to be looked up based on that name in a Handle System directory.

Digital Rights Management (DRM)

Digital Rights Management (DRM) involves the description, layering, analysis, valuation, trading, and monitoring of an owner's property rights to an asset. DRM covers the management of the digital rights to the physical manifestation of a work (e.g., a textbook) or the digital manifestation of a work (e.g., a Web page). DRM also covers the management of

an asset whether the asset has a tangible or an intangible value. Current DRM systems include languages for describing the terms and conditions for use of an asset, tracking asset usage by enforcing controlled environments or encoded asset manifestations, and closed architectures for the overall management of the digital rights. Since the current DRM systems typically rely upon location-based identifiers such as the URL, the system is limited by the inflexibility of the location-based identifier.

Thus, there is a need for an apparatus, method, and system for reliably accessing a digitized work of authorship that is protected by a DRM system. The apparatus, method, and system disclosed herein improves the durability of a DRM system, provides additional capability to both the DRM customer and the content publisher, and promotes the growth of electronic commerce.

SUMMARY OF THE INVENTION

Digital rights management (DRM) and content distribution systems need to reference unique works of authorship to facilitate distribution, access control, and usage tracking and reporting of the works. The apparatus, method, and system disclosed herein is a DRM and content distribution system that uses the digital object identifier (DOI) as a unique identifier for the works of authorship that are the subject of transactions within the system and that travel with the instantiations of the works of authorship.

A method of accessing a digital work from a computer is disclosed. The method associates at least one usage right with the digital work to create a protected digital work. The usage rights include displaying the digital work, copying the digital work, forwarding the digital work to another computer, or printing the digital work. The method selects a unique identifier such as a DOI for the digital work and stores the protected digital work and the

unique identifier in a directory such as a library of digital works of authorship or a portion of a peer-to-peer network. The method issues a query from the computer to the directory to generate a result set that includes the unique identifier. The method uses the unique identifier to retrieve the protected digital work from the directory.

In another embodiment, the method encrypts the protected digital work using a prior art encryption algorithm and/or wraps the protected digital work with a secure container. The secure container can include a digital watermark using a prior art watermarking algorithm or can use a watermarking algorithm that includes the unique identifier associated with the digital work.

In another embodiment, the method stores metadata that describes the protected digital work and includes the metadata in the query from the computer. Furthermore, the query can originate from either a computer coupled to a user or from a third party such as a content distributor, a content syndicator, or a content aggregator.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying figures best illustrate the details of the apparatus, method, and system, for integrating digital object identifiers into a digital rights management system, both as to its structure and operation. Like reference numbers and designations in these figures refer to like elements.

Figure **1** illustrates one example embodiment incorporated into a Digital Rights Management (DRM) controller.

Figures **2** and **3** illustrate URL addressing across a communications network with moving information.

Figure **4** illustrates accessing of information through DOIs.

Figures **5** and **6** provide an overview of a Handle.

Figures **7** and **8** provide an overview of the resolution mechanism for allowing users to access desired information.

Figure **9** provides an overview of an exemplary sequence of actions that a user performs to access information using DOIs.

Figure **10** provides a more complete overview of an exemplary sequence of actions that users perform to access content information.

Figure **11** illustrates an exemplary mechanism for accessing information over a communications network.

Figure **12** provides an overview of another embodiment of exemplary mechanisms for retrieving information over a communications network.

Figure **13** provides an overview of an exemplary DOI registration system.

Figure **14** is a functional block diagram that illustrates the interaction between the parties involved in a traditional digital rights management scenario that uses digital object identifiers to increase the durability of the system.

Figure **15** is a functional block diagram that illustrates the integration of a watermark into the digital rights management scenario shown in Figure **14**.

Figure **16A** is a flow diagram of an embodiment of the watermarking process shown in Figure **15** that results in a user opening a protected digital work.

Figure **16B** is a flow diagram of an embodiment of the watermarking process shown in Figure **15** that results in a user accessing a hacked digital work.

Figure **16C** is a flow diagram of an embodiment of the watermarking process shown in Figure **15** that results in a user accessing an informally distributed digital work.

Figure **17** is a functional block diagram that illustrates the integration of a validation architecture into the digital rights management scenario shown in Figure **14**.

Figures **18** and **19** illustrate a schematic diagram of one non-limiting example embodiment of an interactive interface multiple resolution menu facility (MRMF)

DETAILED DESCRIPTION OF THE INVENTION

Digital Rights Management Controller

Figure 1 illustrates one example embodiment incorporated into Digital Rights Management System (DRMS) controller **101**. In this embodiment, DRM controller **101** may serve to register, resolve, process, store, update, and validate Handles and any associated information, and/or the like.

In one embodiment, DRM controller **101** may be connected to and/or communicate with entities such as, but not limited to, one or more users from user input devices **111**, peripheral devices **112**, communications network **113**, and/or the like. DRM controller **101** may even be connected to and/or communicate with cryptographic processor device **128**.

DRM controller **101** may typically be based on common computer systems that may comprise components such as, but not limited to, conventional computer systemization **102** connected to memory **129** and/or the like.

Conventional Computer Systemization

Conventional computer systemization **102** may comprise clock **130**, central processing unit (CPU) **103**, read only memory (ROM) **106**, random access memory (RAM) **105**, interface bus **107** and/or the like. Conventionally, although not necessarily, the elements that comprise conventional computer systemization **102** are all interconnected and/or communicating through system bus **104**. Clock **130** typically has a crystal oscillator and

provides a base signal. Clock **130** is typically coupled to system bus **104** and various means that will increase or decrease the base operating frequency for other components interconnected in the computer systemization. Clock **130** and various components in a computer systemization drive signals embodying information throughout the system. Such transmission and reception of signals embodying information throughout a computer systemization may be commonly referred to as communications. These communicative signals may further be transmitted, received, and the cause of return and/or reply signal communications beyond the instant computer systemization to communications networks, input devices, other computer systemizations, peripheral devices, and/or the like. Optionally, cryptographic processor **126** may similarly be connected to system bus **104**. It is to be understood that any of the above components may be connected directly to one another, connected to the CPU **103**, and/or organized in numerous variations employed as exemplified by various computer systems.

CPU **103** comprises at least one high-speed data processor adequate to execute program modules for executing user and/or system-generated requests. CPU **103** may be a microprocessor such as, but not limited to, the Intel Pentium Processor and/or the like. CPU **103** interacts with memory through signal passing through conductive conduits to execute stored program code according to conventional data processing techniques. Such signal passing facilitates communication within the DQAS controller and beyond through various interfaces.

Interface Adapters

Interface bus(ses) **107** may accept, connect, and/or communicate to a number of interface adapters, conventionally although not necessarily in the form of adapter cards, such

as, but not limited to, input output (I/O) interfaces **108**, storage interfaces **109**, network interfaces **110**, and/or the like. Optionally, cryptographic processor interfaces **127** similarly may be connected to the interface bus. The interface bus provides for the communications of interface adapters with one another as well as with other components of the computer systemization. Interface adapters are adapted for a compatible interface bus. Interface adapters conventionally connect to the interface bus via a slot architecture. Conventional slot architectures may be employed, such as, but not limited to, Accelerated Graphics Port (AGP), Card Bus, (Extended) Industry Standard Architecture ((E)ISA), Micro Channel Architecture (MCA), NuBus, Peripheral Component Interconnect (PCI), Personal Computer Memory Card International Association (PCMCIA), and/or the like.

Storage interfaces **109** may accept, communicate, and/or connect to a number of storage devices such as, but not limited to, storage devices **114**, removable disc devices, and/or the like. Storage interfaces may employ connection protocols such as, but not limited to, (Ultra) Advanced Technology Attachment (Packet Interface) ((Ultra) ATA(PI)), (Enhanced) Integrated Drive Electronics ((E)IDE), Institute of Electrical and Electronics Engineers (IEEE) 1394, fiber channel, Small Computer Systems Interface (SCSI), Universal Serial Bus (USB), and/or the like.

Network interfaces **110** may accept, communicate, and/or connect to communications network **113**. Network interfaces may employ connection protocols such as, but not limited to, direct connect, Ethernet (thick, thin, twisted pair 10/100/1000 Base T, and/or the like), Token Ring, wireless connection such as IEEE 802.11b, and/or the like. Communications network **113** may be any one and/or the combination of a direct interconnection, the Internet, Local Area Network (LAN), Metropolitan Area Network (MAN), Operating Missions as

Nodes on the Internet (OMNI), a secured custom connection, Wide Area Network (WAN), wireless network (e.g., employing protocols such as, but not limited to a Wireless Application Protocol (WAP), I-mode, and/or the like), and/or the like. A network interface may be regarded as a specialized form of an input/output interface.

Input Output (I/O) interfaces **108** may accept, communicate, and/or connect to user input devices **111**, peripheral devices **112**, cryptographic processor devices **128**, and/or the like. I/O may employ connection protocols such as, but not limited to, Apple Desktop Bus (ADB); Apple Desktop Connector (ADC), audio based on analog, digital, monaural, RCA, stereo, and/or the like, IEEE 1394, infrared, joystick, keyboard, midi, optical, PC AT, PS/2, parallel based on radio, serial, USB, video interface based on BNC, composite, digital, RCA, S-Video, VGA, and/or the like, wireless, and/or the like. A common output device is a video display, which typically comprises a CRT or LCD based monitor with an interface (e.g., VGA circuitry and cable) that accepts signals from a video interface. The video interface composites information generated by a computer systemization and generates video signals based on the composited information. Typically, the video interface provides the composited video information through a video connection interface that accepts a video display interface (e.g., a VGA connector accepting a VGA display cable).

User input devices **111** may be card readers, dongles, finger print readers, gloves, graphics pads, joysticks, keyboards, mouse (mice), trackballs, trackpads, retina readers, and/or the like.

Peripheral devices **112** may be connected and/or communicate with or to I/O and/or with or to other facilities of the like such as network interfaces, storage interfaces, and/or the like). Peripheral devices may be cameras, dongles (for copy protection, ensuring secure

transactions as a digital signature, and/or the like), external processors (for added functionality), goggles, microphones, monitors, network interfaces, printers, scanners, storage devices, visors, and/or the like.

Cryptographic units such as, but not limited to, microcontrollers, processors **126**, interfaces **127**, and/or devices **128** may be attached, and/or communicate with the DRM controller. An MC68HC16 microcontroller, commonly manufactured by Motorola Inc., may be used for and/or within cryptographic units. Equivalent microcontrollers and/or processors may also be used. The MC68HC16 microcontroller utilizes a 16-bit multiply-and-accumulate instruction in the 16 MHz configuration and requires less than one second to perform a 512-bit RSA private key operation. Cryptographic units support the authentication of communications from interacting agents, as well as allowing for anonymous transactions. Cryptographic units may also be configured as part of CPU **103**. Other commercially available specialized cryptographic processors include VLSI Technology's 33 MHz 6868 or Semaphore Communications' 40 MHz Roadrunner 284.

Memory

Storage device **114** may be any conventional computer system storage. Storage devices may be a fixed hard disk drive, and/or other like devices. However, it is to be understood that a DRM controller and/or a computer systemization may employ various forms of memory **129**. For example, a computer systemization may be configured wherein the functionality of on-chip CPU memory (e.g., registers), RAM, ROM, and any other storage devices are provided by a paper punch tape or paper punch card mechanism. Of course, such an embodiment is not preferred and would result in an extremely slow rate of operation. In a typical configuration, memory **129** will include ROM, RAM, and storage device **114**.

Generally, any mechanization and/or embodiment allowing a processor to affect the storage and/or retrieval of information is regarded as memory **129**. Thus, a computer systemization generally requires and makes use of memory. Since memory is a fungible technology and resource, any number of memory embodiments may be employed in lieu of or in concert with one another.

Module Collection

Storage device **114** may contain a collection of program and/or database modules and/or data such as, but not limited to, operating system module **115** (i.e., operating system), information server module **116** (i.e., information server) user interface module **117** (i.e., user interface), web browser module **118** (i.e., web browser), DRM database **119**, cryptographic server module **120** (i.e., cryptographic server), Information Access Multiple Resolution Server (IAMRS) module **125**, and/or the like (i.e., collectively, a module collection). These modules may be stored and accessed from the storage devices and/or from storage devices accessible through an interface bus. Although non-conventional software modules such as those in the module collection, typically and preferably, are stored in a local storage device **114**, they may also be loaded and/or stored in memory such as peripheral devices, RAM, remote storage facilities through a communications network, ROM, various forms of memory, and/or the like.

Operating System

Operating system module **115** is executable program code facilitating the operation of a DRM controller. Typically, the operating system facilitates access of I/O, network interfaces, peripheral devices, storage devices, and/or the like. The operating system preferably is a conventional product such as Apple Macintosh OS X Server, AT&T Plan 9,

Microsoft Windows NT Server, Unix, and/or the like operating systems. Preferably, the operating system is highly fault-tolerant, scalable, and secure. An operating system may communicate to and/or with other modules in a module collection, including itself, and/or facilities of the like. Conventionally, the operating system communicates with other program modules, user interfaces, and/or the like. For example, the operating system may contain, communicate, generate, obtain, and/or provide program module, system, user, and/or data communications, requests, and/or responses. The operating system, once executed by CPU **103**, may enable the interaction with communications networks, data, I/O, peripheral devices, program modules, memory, user input devices, and/or the like. Preferably, the operating system provides communications protocols that allow the DRM controller to communicate with other entities through communications network **113**. Various communication protocols may be used by the DRM controller as a subcarrier transport mechanism for interacting with the Handle System, such as, but not limited to, multicast, TCP/IP, UDP, unicast, and/or the like.

Information Server

Information server module **116** is stored program code that is executed by CPU **103**. The information server may be a conventional Internet information server such as, but not limited to, Microsoft's Internet Information Server and/or the Apache Software Foundation's Apache. Preferably, the information server allows for the execution of program modules through facilities such as C++, Java, JavaScript, ActiveX, Common Gateway Interface (CGI) scripts, Active Server Page (ASP), and/or the like. Preferably the information server supports secure communications protocols such as, but not limited to, File Transfer Protocol (FTP); HyperText Transfer Protocol (HTTP); Secure Hypertext Transfer Protocol (HTTPS), Secure

Socket Layer (SSL), and/or the like. Conventionally, an information server provides results in the form of web pages to web browsers, and allows for the manipulated generation of the web pages through interaction with other program modules. After a DNS resolution portion of an HTTP request is resolved to a particular information server, the information server resolves requests for information at specified locations on a DRM controller based on the remainder of the HTTP request. For example, a request such as http://123.124.125.126/myInformation.html might have the IP portion of the request "123.124.125.126" resolved by a DNS server to an information server at that IP address; that information server might in turn further parse the http request for "/myInformation.html" portion of the request and resolve it to a location in memory containing the information "myInformation.html." An information server may communicate to and/or with other modules in a module collection, including itself, and/or facilities of the like. Most frequently, the information server communicates with operating systems, other program modules, user interfaces, web browsers, and/or the like. An information server may contain, communicate, generate, obtain, and/or provide program module, system, user, and/or data communications, requests, and/or responses.

User Interface

User interface module **117** is stored program code that is executed by CPU **103**. Preferably, the user interface is a conventional graphic user interface as provided by, with, and/or atop operating systems and/or operating environments such as Apple Macintosh OS, e.g., Aqua, Microsoft Windows (NT), Unix X Windows (KDE, Gnome, and/or the like), and/or the like. The user interface may allow for the display, execution, interaction, manipulation, and/or operation of program modules and/or system facilities through textual

and/or graphical facilities. The user interface provides a facility through which users may affect, interact, and/or operate a computer system. A user interface may communicate to and/or with other modules in a module collection, including itself, and/or facilities of the like. Most frequently, the user interface communicates with operating systems, other program modules, and/or the like. The user interface may contain, communicate, generate, obtain, and/or provide program module, system, user, and/or data communications, requests, and/or responses.

Web Browser

Web browser module **118** is stored program code that is executed by CPU **103**. Preferably, the web browser is a conventional hypertext viewing application such as Microsoft Internet Explorer or Netscape Navigator (preferably with 128bit encryption by way of HTTPS, SSL, and/or the like). Some web browsers allow for the execution of program modules through facilities such as Java, JavaScript, ActiveX, and/or the like. In one embodiment, web browsers are Handle-enabled by way of a browser plug-in software such as the Handle System plug-in available from www.cnri.org. In an alternative embodiment Handle support is integrated into the web browser. Web browsers and like information access tools may be integrated into PDAs, cellular telephones, and/or other mobile devices. A web browser may communicate to and/or with other modules in a module collection, including itself, and/or facilities of the like. Most frequently, the web browser communicates with information servers, operating systems, integrated program modules (e.g., plug-ins), and/or the like; e.g., it may contain, communicate, generate, obtain, and/or provide program module, system, user, and/or data communications, requests, and/or responses. Of course, in place of a web browser and information server, a combined application may be developed to perform

similar functions of both. The combined application would similarly affect the obtaining and the provision of information to users, user agents, and/or the like from DRM enabled nodes. The combined application may be nugatory on systems employing standard web browsers. Such a combined module could be configured to communicate directly with the DRM without an intermediary information server to further enhance security.

Digital Object Identifiers (DOIs)

DOIs overcome many of the shortcomings of Internet Protocol (IP) and other location-based addressing schemes. DOIs enable access to information over a communications network by providing a persistent identifier for information that may be regularly relocated. DOIs overcome the limitations of network addressing schemes limited to addressing locations by providing a mechanism to associate identifiers with information through an added level of indirection instead of associating identifiers with locations.

DRM Database

DRM database module **119** may be embodied in a database that is stored program code that is executed by the CPU **103** and its stored data; the stored program code portion configuring the CPU **103** to process the stored data. Preferably, the database is a conventional, fault tolerant, relational, scalable, secure database such as Oracle or Sybase. Relational databases are an extension of a flat file. Relational databases consist of a series of related tables. The tables are interconnected via a key field. Use of the key field allows the combination of the tables by indexing against the key field, that is, the key fields act as dimensional pivot points for combining information from various tables. Relationships generally identify links maintained between tables by matching primary keys. Primary keys represent fields that uniquely identify the rows of a table in a relational database. More

precisely, they uniquely identify rows of a table on the "one" side of a one-to-many relationship.

Alternatively, the DRM database may be implemented using various standard data structures, such as an array, hash, (linked) list, struct, and/or the like. Such data structures may be stored in memory and/or in (structured) files. If the DRM database is implemented as a data structure, the use of the DRM database may be integrated into another module such as the DRM module. Databases may be consolidated and/or distributed in countless variations through standard data processing techniques. Portions of databases, e.g., tables, may be exported and/or imported and thus decentralized and/or integrated. In one non-limiting example embodiment, the DRM database **119** includes tables such as but not limited to a UNI (e.g., Handle, DOI and/or other UNIs) table **119a**, URL table **119b**, metadata table **119c**, multiple resolution table **119d**, policy table **119e**, and/or the like. All the tables may be related by (enhanced) DOI key field entries as they are unique. In an alternative embodiment, these tables have been decentralized into their own databases and their respective database controllers (i.e., individual database controllers for each of the above tables). Of course, employing standard data processing techniques, one may further distribute the databases over several computer systemizations and/or storage devices. Similarly, configurations of the decentralized database controllers may be varied by consolidating and/or distributing the various database modules **119a-e**. DRM database **119** may be configured to keep track of user requests and various transactions tracking via database controllers.

DRM database **119** may communicate to and/or with other modules in a module collection, including itself, and/or facilities of the like. Most frequently, DRM database **119** communicates with a DRM module, other program modules, and/or the like. The database

may contain, retain, and provide information regarding other nodes and data.

Cryptographic Server

Cryptographic server module **120** is stored program code that is executed by the CPU **103**, cryptographic processor **126**, cryptographic processor interface **127**, cryptographic processor device **128**, and/or the like. Preferably, cryptographic processor interfaces will allow for expedition of encryption and/or decryption requests by the cryptographic module. Cryptographic server module **120** may alternatively run on a conventional CPU. Preferably, cryptographic server module **120** allows for the encryption and/or decryption of provided data. Preferably, cryptographic server module **120** allows for both symmetric and asymmetric (e.g., Pretty Good Protection (PGP)) encryption and/or decryption. Preferably, cryptographic server module **120** allows conventional cryptographic techniques such as, but not limited to, digital certificates (e.g., X.509 authentication framework), digital signatures, dual signatures, enveloping, password access protection, public key management, and/or the like. Preferably, cryptographic server module **120** will facilitate numerous (encryption and/or decryption) security protocols such as, but not limited to, checksum, Data Encryption Standard (DES), Elliptical Curve Encryption (ECC), International Data Encryption Algorithm (IDEA), Message Digest 5 (MD5, which is a one way hash function), passwords, RC5 (Rivest Cipher), Rijndael, RSA (which is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman), Secure Hash Algorithm (SHA), Secure Socket Layer (SSL), Secure Hypertext Transfer Protocol (HTTPS), and/or the like. The cryptographic module facilitates the process of "security authorization" whereby access to a resource is inhibited by a security protocol wherein the cryptographic module effects authorized access to the secured resource. A cryptographic

module may communicate to and/or with other modules in a module collection, including itself, and/or facilities of the like. Preferably, cryptographic server module **120** supports encryption schemes allowing for the secure transmission of information across a communications network to enable a DRM module to engage in secure transactions if so desired by users. The cryptographic module facilitates the secure accessing of resources on DRM and facilitates the access of secured resources on remote systems, that is, it may act as a client and/or server of secured resources. Most frequently, cryptographic server module **120** communicates with information servers, operating systems, other program modules, and/or the like. Cryptographic server module **120** may contain, communicate, generate, obtain, and/or provide program module, system, user, and/or data communications, requests, and/or responses.

Information Access Multiple Resolution Server (IAMRS)

IAMRS module **125** is stored program code that is executed by CPU **103**. Generally, the DRM affects accessing, obtaining and the provision of information, and/or the like between nodes on a communications network. The IAMRS has the ability to resolve UNIs to multiple instantiations and services, depending on the type of inbound request. Generally, the IAMRS acts as a lookup facility to create, maintain, and update associations between a given piece of information, its DOI, its current locations, and pointers to associated services. The IAMRS coordinates with the DRM database to identify nodes that may be useful for improving data transfer for requested information, for resolving to various formats of the requesting information, providing an enhanced mechanism to create queries regarding the information, and/or the like. An IAMRS enabling access of information between nodes may be developed by employing standard development tools such as, but not limited to, C++, shell

scripts, Java, Javascript, SQL commands, web application server extensions, Apache modules, Perl scripts, binary executables, and/or other mapping tools, and/or the like. In one non-limiting example embodiment, the IAMRS server employs a cryptographic server to encrypt and decrypt communications. The IAMRS may service requests, update association information for UNIs, and much more. A DRM module may communicate to and/or with other modules in a module collection, including itself, and/or facilities of the like. Most frequently, the IAMRS module communicates with a DRM database, operating systems, other program modules, and/or the like. The IAMRS may contain, communicate, generate, obtain, and/or provide program module, system, user, and/or data communications, requests, and/or responses.

Digital Rights Management Server (DRMS)

DRM module **135** is stored program code that is executed by CPU **103**. DRM module **135** can operate in a stand-alone mode separate from a UNI registration system such as the Information Access Registration System (IARS). DRM module **135** can generate tags that are embedded into information represented by the DOI so that the information may be validated. DRM module **135** coordinates with the DRM database to identify nodes that may be useful for validating UNI and associated information integrity, improving data transfer for requested information, resolving to various formats of the requesting information, providing an enhanced mechanism to create queries regarding the information, and/or the like. A DRM enabling access of information between nodes may be developed by employing standard development tools such as, but not limited to, C++, shell scripts, Java, Javascript, SQL commands, web application server extensions, Apache modules, Perl scripts, binary executables, and/or other mapping tools, and/or the like. In one non-limiting example

embodiment, DRM module **135** employs a cryptographic server to encrypt and decrypt communications. DRM module **135** may service requests, redirect requests, update association information for UNIs, and much more. DRM module **135** may also communicate to and/or with other modules in a module collection, including itself, and/or facilities of the like. Most frequently, DRM module **135** communicates with a DRM database, an IAMRS module, and IARS module, operating systems, other program modules, and/or the like. DRM module **135** may contain, communicate, generate, obtain, and/or provide program module, system, user, and/or data communications, requests, and/or responses.

Distributed DRMS

The functionality of any of the DRM node controller components may be combined, consolidated, and/or distributed in any number of ways to facilitate development and/or deployment. Similarly, the module collection may be combined in any number of ways to facilitate deployment and/or development. To accomplish this, one must simply integrate the components into a common code base or in a facility that can dynamically load the components on demand in an integrated fashion.

The module collection may be consolidated and/or distributed in countless variations through standard data processing and/or development techniques. Multiple instances of any one of the program modules in the program module collection may be instantiated on a single node, and/or across numerous nodes to improve performance through load balancing data processing techniques. Furthermore, single instances may also be distributed across multiple controllers and/or storage devices; e.g., databases.

All program module instances and controllers working in concert may do so through standard data processing communication techniques.

The preferred DRM controller configuration will depend on the context of system deployment. Factors such as, but not limited to, the capacity and/or location of the underlying hardware resources may affect deployment requirements and configuration. Regardless of if the configuration results in more consolidated and/or integrated program modules, results in a more distributed series of program modules, and/or results in some combination between a consolidated and/or distributed configuration, communication of data may be communicated, obtained, and/or provided. Instances of modules (from the module collection) consolidated into a common code base from the program module collection may communicate, obtain, and/or provide data. This may be accomplished through standard data processing techniques such as, but not limited to: data referencing (e.g., pointers), internal messaging, object instance variable communication, shared memory space, variable passing, and/or the like (intra-application communication).

If module collection components are discrete, separate, and/or external to one another, then communicating, obtaining, and/or providing data with and/or to other module components may be accomplished through standard data processing techniques such as, but not limited to, Application Program Interfaces (API) information passage; (distributed) Component Object Model ((D)COM), (Distributed) Object Linking And Embedding ((D)OLE), and/or the like), Common Object Request Broker Architecture (CORBA), process pipes, shared files, and/or the like (inter-application communication). Messages sent between discrete module components for inter-application communication or within memory spaces of a singular module for intra-application communication may be facilitated through the creation and parsing of a grammar. A grammar may be developed by using standard development tools such as lex, yacc, and/or the like, which allow for grammar generation and parsing

functionality, which in turn may form the basis of communication messages within and between modules. Again, the preferable embodiment will depend upon the context of system deployment.

Finally, it is to be understood that the logical and/or topological structure of any combination of the module collection and/or the present invention as described in the figures and throughout are not limited to a fixed execution order and/or arrangement, but rather, any disclosed order is exemplary and all functional equivalents, regardless of order, are contemplated by the disclosure. Furthermore, it is to be understood that such structures are not limited to serial execution, but rather, any number of threads, processes, services, servers, and/or the like that may execute asynchronously, simultaneously, synchronously, and/or the like are contemplated by the disclosure.

IP Addressing

Users access communications networks through addresses. Addresses represent locations. Users traverse locations in a communications network hoping to find information. A common communications addressing scheme employs the IP address. The IP address may be likened to the real world by analogy to a street address. The IP address itself is a sequence of numbers, e.g., 209.54.94.99, and commonly has an associated name, e.g., www.contentdirections.com. A distributed database registry maintains the associated pairs of names and IP addresses and serves to resolve associated names into corresponding IP addresses. This allows people to remember and use names, e.g., www.report.com, instead of being forced to memorize and use a series of numbers, e.g., 209.54.94.99. These distributed databases assisting in the name resolution of IP addresses are commonly referred to as Domain Name Servers (DNS).

It is common for IP addresses to be embodied as Universal Resource Locators (URLs) that append even more navigation information into an address. Users may employ software to access information stored at URLs through the use of HTTP. An example is when a user specifies "http://www.report.com /reports/1999/IncomeStatement.html" in a web browser. Typically this further navigation information, i.e., "/reports/1999/IncomeStatement.html," provides a specific storage location within a computer server. This further navigation location may be likened to a real world address more specific than a street address that includes information such as a company name, department, and room number. This further navigation location is typically not Handled or resolved by DNSs, but instead by an information server at the resolved IP address. For example, an information server at the resolved address of 123.123.123.123 for www.report.com would interpret and return information at a local location of "/reports/1999/IncomeStatement.html" within the server. An Information Server is a means for facilitating communications between a communication network and the computer server at a particular IP address. Commercial examples of an Information Server include Apache. An Information Server may be likened to a mail department for a business that further routes correspondence to appropriate locations within the business.

Figures 2 and 3 illustrate that IP addressing mechanisms do not maintain an association with information as it moves across a communications network. Web page links generally employ HTTP, which in turn relies on IP addressing. Thus, URL links simply point to a location on a communication network and are not necessarily associated with any specific information. For example, a URL link referencing www.news.com will have different information associated between the URL and the information made available at the www.news.com location as information at the location is updated daily. In many instances,

locations themselves may disappear as companies move information, move their operations, go out of business, etc.

For example, a report entitled "Company Sales for 1999" **222** existing at a location www.report.com/1999/Report.html **208** may be moved to www.report-archives.com/1999/Old-report.html **310**, e.g., because the information was sold from one entity to another, archived, or for many other reasons. The report at www.report.com/1999/Report.html **208** may have had 5 million web pages and URL links referencing the location **244**, and when users attempt to access the information they may well receive a "404 File not found" error **309** because that location no longer exists and/or no longer contains the desired information. The error results because the DNSs were designed to always resolve users' requests to a location and because DNSs are not designed to maintain an association between URLs and a specific instantiation of information.

Figure **2** depicts web page **201**, user entered address **202**, document **203**, and memory device **204** each employing URLs and consequently IP addressing in an attempt to reference a piece of information (the report "Company Sales for 1999" **222**). Then in Figure **2**, the information **222** is moved from its original location **208** (for example at www.report.com/1999/Report.html) to a new location **310** of Figure **3** (for example www.report.com/1999/Archives.html). In Figure **3**, this results in breaking **301-304** all the URLs **244** referencing the location and produces the dreaded "404 file not found" error **309** for all users and URLs making reference to the location (www.report.com/1999/Report.html **208**).

Handle System

Once a piece of information has been assigned a DOI and has been made available, the DOI system needs to be able to resolve what the user of the DOI wants to access. The technology that is used to manage the resolution of DOIs is better known as the "Handle System," and will be described in more detail below. THE DOI HANDBOOK provides a general overview of basic DOIs. In a nutshell, the Handle System includes an open set of protocols, a namespace, and an implementation of the protocols. The protocols enable a distributed computer system to store Handles (such as DOIs) of digital content and resolve those Handles into the information necessary to locate and access the content, to locate and access information related to the content, or to locate and access (i.e., provide an interface to) services associated with the content. This associated information can be changed as needed to reflect the current state of the identified content without changing the DOI, thus allowing the name of the item to persist over changes of location and other state information. Combined with a centrally administered DOI registration agency, the Handle System provides a general-purpose, distributed global naming service for the reliable management of information and services on networks over long periods of time. It is important to note that throughout the present disclosure that "source," "content" and/or "information" made accessible through the DOI system may comprise any identifiable content, source, information, services, transactions, and work of authorship, including articles, books, intangible objects, music albums, people, tangible physical objects, and/or the like further including selected discrete portions and/or combinations thereof. The accessible information may be a URL to an application that initiates a service, a transaction, provides a selection mechanism, and/or the like. In one non-limiting example, the DOI may even be associated

with information identifying a human being such as a social security number, telephone number, and/or the like. In another non-limiting example, the DOI may be associated with software modules, programming "objects," or any other network-based resource. Furthermore, a DOI can be used to represent most anything including the online representation of physical products (e.g., items currently identified by UPC or bar codes). In such an example, DOIs could resolve to the manufacturer's catalog page describing or offering the product, or even, in a multiple-resolution scenario, offer all services related to the object such as where to go to get the item repaired; where to find replacement parts; what the new or replacement product is; what kinds of pricing or leasing options are available, etc. Other example embodiments implementing DOIs include: representing different modules of software that may operate in distributed fashion across a communications network; telephone numbers for Voice-over-IP technology; gene sequences; medical records and/or other permanent records (DOIs will be especially useful with permanent records protected via encryption and/or other method that might invoke a certificate or decryption key); and/or the like. Another example embodiment for a DOI is to represent the permanent location of a temporary and/or dynamic value such as, but not limited to a current stock quote; current bid and offer prices (for stocks and/or any other kind of auction and/or exchange); a company's current annual report (versus different DOIs for different prior-year annual reports); and/or the like.

Users may access information through Digital Object Identifiers (DOIs). DOIs are associated with (i.e., are names for) information itself. DOIs are instances of "Handles" and operate within the framework of the "Handle system." A DOI allows for access to persistently associated information. The DOI is a string of characters followed by a separator

further followed by a string of characters, e.g., 10.1065/abc123def. It should be noted and re-emphasized that although the present disclosure may make mention of specific sub-types of UNIs such as "URNs," "DOIs" and "Handles," the present disclosure applies equally well to the more generic types of UNIs, and as such, the present disclosure should be regarded as applying to UNIs in general where any UNI sub-type is mentioned, unless stated otherwise. Furthermore, although the Handle System, DOIs, and their supporting technologies and conventions, which are in use today, are a contemplated forum for the present invention, it should be noted that it is contemplated that the present invention may be applied to other forums based upon current and yet to be conceived conventions and systems.

DOIs

Users employing DOIs to access information know they will resolve and access only associated information. In contrast to URLs that reference locations, DOIs are names for information, which can be used to look up that information's location and other attributes, as well as related services. It is envisioned that information may be any information as well as any computer-readable files, including e-books, music files, video files, electronic journals, software, smaller portions and/or combinations of any of the aforementioned content as well. It should be noted that since the electronic content will be made available over a communications network, hereinafter this application refers to such available information as being published on a communications network.

A DOI is a permanent and persistent identifier given to a piece of information made available on a communications network and registered in an electronic form, so that even if the location (i.e., URL), format, ownership, etc. of the content or associated data changes, users will be able to access the associated data. DOIs, or Handles, may be distributed to users

in lieu of a URL. A user may access information associated with a particular DOI by selecting or entering the DOI in a Handle-enabled web browser much like a URL hyperlink. Many types of browsers may be enabled by way of browser plug-in software such as the Handle System plug-in available from www.cnri.org. Such an attempt to access DOI associated information triggers an automated process to look up a resource's current location. The current location of the resource is associated with the resource's DOI in a centrally managed directory made available by the Handle System, which in turn directs the user (i.e., the user's web browser) to the resource's current location. This direction is often accomplished by returning a current URL associated with the selected DOI and corresponding information.

Figure **4** illustrates the access of information through DOIs in contrast to Figures **2** and **3** above. Initially, the information (report of "Company Sales for 1999" **222**) is given a DOI through a registration process. Instead of employing URLs, users reference **444** the information using the DOI through web pages **401**, typed entry in a web browser **402**, documents **403**, devices **404**, barcodes **406**, and/or the like. When users engage the DOI links **444**, they are resolved in a centralized DOI directory **411** and the requesting users are given a URL link **244** to the information's **222** initial location (www.report.com/1999/Report.html **208**). Upon the information being moved **434** from its initial location (www.report.com/1999/Report.html **208**) to a new location (www.report.com/1999/Archives.html **310**), the publisher of the information **410** would inform the DOI centralized directory **445** of the new location for the information by sending an updated URL **245** referencing the new location. Thereafter, if users **401-404** attempt to access the information through the DOI links **444**, the DOI directory will properly provide the

new location **310** by way of the updated URL **245**.

As noted above, DOIs may not only be used to identify information, but also smaller portions thereof. For example, according to the DOI system, it is possible for a book to have one DOI, while each of its chapters would have other unique DOIs to identify them; furthermore, each figure in the book may have yet other unique DOIs to identify them. In other words, according to the DOI system, it is possible to identify information with variable granularity as desired by the content publishers. Furthermore, it is envisioned that just as Universal Product Codes (commonly expressed as 'bar-codes' on consumer products) allow, for example, a supermarket's cash registers, inventory computers, financial systems, and distributors to automate the supply chain in the physical world, the present disclosure provides a mechanism for employing DOIs to empower all kinds of agents in the world of electronic publishing to automate the sale of digital content (and the licensing of rights to that content) across the Internet in an efficient manner, since each piece of saleable content would have associated with it a globally unique DOI, which could be used as a product identification code in transactions between agents.

Handle Structure

The Handle System employs a pre-determined set of policies for efficient and user-friendly utilization thereof, some of which of which are listed below. The use of the Handle System for DOI resolution should ideally be free to users, with the costs of operation of the system possibly borne by the publishers. All DOIs are to be registered with a global DOI registry. Registrants are responsible for the maintenance of state data and metadata relating to DOIs that they have registered. The syntax of the DOI follows a standardized syntax. In use, the DOI will be an opaque string (dumb number). DOI registration agencies will manage the

assignment of DOIs, their registration and the declaration of the metadata associated with them.

Figure **5** and **6** provide a schematic view of a Handle 600. A Handle **600** has two components, the prefix **501** and the suffix **602**. The prefix **501** and the suffix **502** are separated by a forward slash **507**. The Handle **500** may incorporate any printable characters from almost every major language written or used today. There is no specified limitation on the length of either the prefix **501** or the suffix **502**. As a result, it is envisioned that there are an almost infinite number of Handles available. It is important to ensure that the combination of the prefix **501** and the suffix **502** is unique for supporting the integrity of the Handle System. Thus, the DOI registration agency will award a unique prefix **501** to a publisher. In one embodiment, the registration agency may put the responsibility on these publishers for ensuring that the suffix **502** assigned is unique as well. This may be achieved with a registration tool running on the user's client computer system. In another embodiment, the registration agency will ensure that the suffix **502** is unique by applying various suffix generation algorithms as discussed throughout this disclosure. The Registration Agency and the Handle System administrators will both verify uniqueness of any new Handle before depositing it in the Handle System. The Registration Agency deposits DOI records with the Handle System. The Handle System in turn services DOI resolution requests through a DOI directory.

The prefix **501** itself has two components separated by a prefix separator **506**, which is a period. The first part of the Handle prefix is the Handle type **504**. The second part of the Handle prefix is the Handle creator **505**. The Handle type **504** identifies what type of Handle system is being used. When the Handle type **504** starts with a "10" the Handle is

distinguished as being a DOI as opposed to any other implementation type of the Handle System. The next element of the prefix, separated by a period, is the Handle creator **505**, which is a number (or string of characters) that is assigned to an organization that wishes to register DOIs. Together, these two elements **504** and **505** form the unique publisher prefix portion of the DOI. There is no limitation placed on the number of Handle (or specifically DOI) prefixes that any organization may choose to apply for. As a result, a publishing company, for example, might have a single DOI prefix **501**, or might have a different one for each of its journals, or one for each of its imprints. While generally a prefix **501** may be a simple numeric string, the scope of the Handle System is not limited thereby. Thus, a prefix **501** may also utilize alphabetical characters or any other characters.

The suffix **502** is a unique string of alphanumeric characters, which, in conjunction with a particular prefix **501**, uniquely identifies a piece of information. It should be appreciated that the combination of the prefix **501** for a publisher and the unique suffix **502** provided by the publisher avoids the need for the centralized allocation of DOI numbers. The suffix **502** may be any alphanumeric string that the publisher chooses, so long as it is unique among all suffixes registered in conjunction with the publisher's prefix.

Figure **6** provides a view of another embodiment of the DOI **600**, in which a textbook's ISBN number serves as the suffix **602**. Consequently, where it is convenient, the publisher of the underlying content may choose to select as the suffix **602** any other identification code accorded to the original piece of content.

Enhanced DOI

Figure **5** further illustrates an enhanced DOI **510** grammar. One non-limiting example embodiment of an enhancement to the DOI grammar is embodied as an enhanced prefix **511**.

However, it is fully contemplated that an alternative and/or complimentary enhanced suffix (not illustrated) may be similarly appended to the DOI **500**. The enhanced prefix **511** is comprised of an enhancement grammar target **517** and enhancement separator **514**, which is an "@" symbol, but it is understood any other character may be designated as the enhancement separator. The enhancement grammar target **517** may itself be any string of characters other than the enhancement separator **514**. The enhancement grammar target **517** may be employed for the purpose of having the DOI **500** resolve to multiple versions of a specified information as will be described in greater detail throughout this disclosure. In a further enhanced embodiment, the enhancement grammar target **517** may itself be further comprised of an enhancement grammar verb **512** and enhancement grammar target object **513** separated by an enhancement target separator **516**, e.g., a period. Of course the enhancement target separator **516** may be designated as any character(s). In one example embodiment, the enhancement grammar verb **512** acts as a modifier to select amongst a plurality of multiple resolution targets for a DOI, and the enhancement grammar target object **513** is a value passed to the target object and/or a Handle system resolution server for further action.

Handle System Metadata

Referring again to Figure **5**, DOI **500** is merely an identification number that does not necessarily convey any information about its associated information. As a result, it is desirable to supplement the DOI with additional information regarding the addressed information to enable users to perform efficient and user-friendly searches for retrieving the desired content over a communications network. To allow easy identification of information, the present invention provides for the use of metadata, which is descriptive data about the identified information. While metadata may be any data structure that is associated with a

DOI, according to one embodiment, the metadata will be comprised of a few basic fields that can accurately and succinctly identify the published information. According to this embodiment, the metadata will comprise an identifier associated with the entity from a legacy identifier scheme such as the International Standard Book Number (ISBN) for a book, title of the published content, type of content being published (such as book, music, video, etc.), whether the content is original or a derivation, a primary author of the content, the role of the primary author in creating the content, the name of the publisher, and/or the like. As different types of content may require different metadata for describing it, one aspect of the DOI system envisions the use of different metadata for different types of content.

According to one example embodiment, metadata will be made available to any user of the DOI system to enable them to find the basic description of the entity that any particular DOI identifies. This basic description will allow the user to understand some basic things about the entity that published the content or the content itself.

As a result, to find out what information the DOI identifies, it is desirable to resolve it, and then review associated metadata because the DOI links the metadata with the content it identifies and with other metadata about the same or related content. In one embodiment, the metadata allows for the recognition of the information identified by DOI **500** as well as its unambiguous specification. The metadata will also allow for the interaction between the information and other contents in the network (and with metadata about those entities).

DOI Information Access

Figures **7** and **8** provide an overview of the resolution mechanism for allowing users to access the desired information by merely providing the DOI to the DOI Handle system. Resolution in the present context includes the submitting of an identifier to a network service

and receiving in return one or more pieces of current information related to the identifier. According to one embodiment of the DOI system, shown in Figure 7, user **700** is a general-purpose workstation running a web browser application to point to content identified by DOI **710**. DOI **710** has only one URL associated with it, and must resolve to that URL. As a result, when user **700** makes a request for underlying content identified by a particular DOI **710**, the user is directed to URL **720**, where the desired content lies.

As such, this mechanism allows the location of the information to be changed while maintaining the name of the entity as an actionable identifier. If the publisher changes the location of the content, the publisher must merely update the DOI's entry in the Handle System database to ensure that the existing DOI **710** points to the new location of the content. As a result, while the location of the content has changed, the DOI remains the same and users are able to access the content from its new location by using the existing DOI.

Figure **8** provides an overview of a DOI system where users may use a DOI for resolving a request for one piece of content, out of a plurality of available identical copies of the same piece of content that are identified by the same DOI, as well as the location of data about the piece of content, and services associated with the content (such as purchasing the content). Thus, user **800**, a general-purpose computer, uses a web browser application to provide the necessary DOI **830**. DOI **830** may be structured to describe the type of service desired **835**. As a result, the DOI system is able to resolve the particular piece of content **840** that the user desires to access.

Figure **9** provides an overview of the sequence of actions that a user performs to access information, in accordance with the present invention. Initially, the user launches browser client **900** on computing device **905**, such as personal computer, personal digital

assistant (PDA), and/or the like. The user engages the browser **900** to make a DOI query. The DOI query is forwarded to the DOI Directory Server **910** over a communications network. The system of the DOI Directory Server **910** examines the DOI against the entries stored therein and forwards the appropriate URL to the browser **900** on the user's computer **900**, in a manner that is invisible to the user. As a result, the browser is pointed to the desired content on a server with the appropriate publisher information **920**. Finally, upon receipt of the request from the user's browser, the publisher **920** forwards the desired information to the user, which may be accessed in the browser client **900**.

Figure **10** provides a more complete view of the sequence of actions that a user performs to access content information, as shown in Figure **9**. As noted above, the user launches the browser client **1000** on a computing device **1005**. The user engages the browser **1000** to make a DOI query. The DOI query is forwarded to the DOI Directory Server **1010** over the communications network. The system of the DOI Directory Server **1010** examines the DOI against the entries stored therein. As a result of the checking of the DOI against the entries stored in the DOI Directory Server **1010**, DOI Directory Server **1010** determines where the DOI must lead the user **1025**. The appropriate URL for the content is automatically forwarded to the user's browser **1000**, without any intermediate intervention or action by the user. As a result, browser **1000** is pointed to the appropriate publisher **1020** whose server is addressed by the underlying URL. The URL is used by the publisher's server **1020** to determine the exact location for content desired by the user, and the publisher's server **1020** forwards the appropriate content **1030** to the user.

Figure **11** provides an overview of some of the exemplary mechanisms for accessing information over a communications network by resolving a DOI to obtain the URL where the

desired content is located, in accordance with the present invention. According to one embodiment, the user may directly provide the DOI and the DOI system retrieves and forwards the appropriate content to the user by simply linking to the appropriate URL. According to another embodiment, the user may provide information related to some of the fields included in the metadata, whereupon a DOI lookup service identifies the appropriate DOI, which in turn may be resolved to the desired content's location. As shown in Figure **11**, according to one embodiment, a search engine **11010** may be provided to a user. In one embodiment, the search engine is offered and disposed in communication with the registration agency's DOI and metadata database. In an alternative embodiment, a search engine such as www.google.com may be adapted to submit queries to the registration agency's databases. The user searches for the appropriate DOI by providing some identifying information to the search engine **11010**. The search engine **11010** uses the identifying information provided and searches a database of metadata to retrieve the DOI associated with the provided metadata information. Thus, the user conducting the search may be presented with returned DOIs from the metadata database and/or URLs resolved from said returned DOIs. The retrieved DOI is sent to the DOI directory **11011**, which resolves the URL wherein the desired content is located by a publisher **11040**. Finally, the user's browser is pointed to the appropriate content **11060**.

According to another embodiment, the user may provide DOI **11015** in address window **11020** of browser **11025**. If the user's web browser is not capable of natively processing DOIs, then DOI **11015** may contain the address of a proxy server for DOI directory **11011**, which in Figure **11** is "dx.doi.org." As a result, the browser is pointed to the DOI directory **11011** located at dx.doi.org, which resolves the URL at which the desired

content is located by a publisher **11040** and points the user's browser thereto.

According to another embodiment, the DOI may be embedded in a document or some form of information **11030**, whereupon clicking the DOI directs the user to the appropriate DOI directory **11011**, which determines the URL at which the desired content is located and points the user's browser thereto.

According to another embodiment, the DOI may be provided on memory **11040**, such as a CD-ROM or a floppy disk, whereupon the memory may automatically, or upon being activated, direct the user to the appropriate DOI directory **11011**, which resolves the URL at which the desired content is located and points the user's browser thereto.

According to yet another embodiment, the DOI may be provided in printed form to a user, who enters the DOI manually as above or by way of optical and/or mechanical peripheral input device.

Figure **12** provides an overview of another embodiment of the exemplary mechanisms for retrieving information over a communications network, whereupon the DOI system resolves a DOI to obtain the URL where the desired information is located. According to this embodiment, a plurality of DOI directories **1210** exist as a distributed DOI directory and form a Handle System **1200**. In one embodiment, the distributed DOI directory acts and responds to requests as if it were a singular directory **11011**. Otherwise resolutions take place similarly as in Figure **11**.

Figure **13** provides an overview of an exemplary DOI system, in accordance with the present invention, wherein the publishers, the DOI registration service and the Handle System collaborate together to create an efficient DOI system. The prefix holder **1355** may submit information to a DOI registration service **1300** comprising DOI **1342** and associated metadata

1366. The prefix holder who has already been assigned a unique prefix **501**, requests that a suffix **502** be assigned to a piece of content **1366**. The registration service **1300** is responsible for parsing and/or reformatting the user's streams of submitted information **1342**, **1366** for subsequent deposit in a Handle system **1350** and/or metadata database **1310**. As noted above, the scope of the content that can be addressed using a DOI is unlimited. As a result, the content **1366** may comprise any information and work of authorship, including articles, books, music albums, or selected discrete portions thereof. In addition to providing DOI **500**, the publisher **1342** collects metadata for the content **1366**. The metadata may comprise the content's DOI **500**, a DOI genre, an identifier, title, type, origination, primary agent, agent's role, and/or the like. It may also comprise listings of associated services having to do with the identified piece of content offered by various parties, such as the locations of web pages where a piece of content may be purchased online.

Once the publisher **1342** has assigned the suffix **502** to the content **1366** and collected the necessary metadata, the DOI **500** and the metadata are transmitted to the DOI registration service **1300**. The DOI registration service **1300** maintains a database of DOIs **500**, metadata of all the registered content **1366**, as well as the URL at which the content **1366** is located. According to the present invention, the DOI registration service **1300** forwards the metadata to a metadata database **1310**, **119c** of Figure **1**, which may or may not be integrally maintained by the DOI registration service **1300**.

The DOI registration service **1300** may use the collected metadata for providing it to other data services **1320** or for providing value-added resources **1330** to the users. In addition, the DOI registration service **1300** sends the appropriate DOI Handle data to the Handle System **1350**, which may comprise a plurality of DOI Directory Servers **1341**.

Digital Rights Management

Figure **14** is a functional block diagram that illustrates the interaction between the parties involved in a traditional digital rights management (DRM) scenario. A traditional DRM scenario begins with publisher **1410** creating or acquiring a digital work that requires protection. Work **1411** is one example of the digital asset. Publisher **1410** sends work **1411** to DRM packaging software **1412** and specifies the rights to associate with work **1411**. These rights restrict the actions that customer **1450** can perform and include, but are not limited to, allowing the customer to read the work, copy the work, forward the work to another customer, and print the work. These rights may also be time-based (e.g. allowing any of the aforementioned actions for a specified period of time such as for two weeks, or from a certain date to another date). These rights may also be granted for a specified number of events (e.g., allowing the customer to access the content for reading 20 times only, or allowing the customer to print a pre-specified number of copies, or allowing the customer to forward the content to a certain number of recipients, or allowing the customer to forward to any number of recipients but allowing access only to the first 20 recipients by requiring all recipients to secure access rights from a central server which has a counter granting access only to the first 20 requestors). These rights may also be associated with various sales promotions, product or service bundlings, or discounts and the like. There are countless variations, combinations and permutations of these rights which may be assigned by Publisher **1410**. Publisher **1410** can specify these rights independently of one another. After the rights are specified, DRM packaging software **1412** may forward protected work **1413** to secure wrapping and encryption **1414** to encrypt the contents of work **1413** and place work in a secure container. The wrapped and secure work is returned to the publisher as secure work **1415**. It is to be

understood that publisher **1410**, DRM packaging software **1412**, and secure wrapping and encryption **1414** can perform the functions described above on either a single computer or a distributed network of computers. Furthermore, it is to be understood that the functions performed by DRM packaging software **1412** and secure wrapping and encryption **1414** can be performed on the behalf of publisher **1410** by an entity other than publisher **1410**. Furthermore, it is to be understood that the functions described above may be performed by different software modules or by software modules which combine these various functions together or with other related or unrelated functions.

Publisher **1410** stores secure work **1415** on content hosting **1420** database. In addition, data that describes secure work **1415** is stored on metadata database **1422**. It is to be understood that publisher **1410**, content hosting **1420**, and metadata database **1422** can perform the functions described above on either a single computer or a distributed network of computers. Furthermore, it is to be understood that the functions performed by DRM content hosting **1420** and metadata **1422** can be performed by an entity other than publisher **1410**.

Customer **1450** obtains a copy of secure work **1415** by a means of digital distribution. Customer **1450** may visit the web site for publisher **1410** to download a copy of secure work **1415**. Alternatively, customer **1450** may browse an index or library catalog and happen across a link to secure work **1415** at either the web site for publisher **1410** or a mirror web site hosted by an entity other than publisher **1410**. Or, customer **1450** may receive secure work **1415** directly from another customer, that is, through "superdistribution". The digital asset is useless to customer **1450** because secure work **1415** is securely wrapped and encrypted by publisher **1410**, as described above.

When customer **1450** attempts to access secure work **1415**, a connection will be

established to rights clearinghouse **1430**. Rights clearinghouse **1430** checks the user identification associated with secure work **1415**, determines the rights that publisher **1410** associated with secure work **1415**, and takes payment for using secure work **1415** from customer **1450**. Rights clearinghouse **1430** has a relationship established with electronic commerce vendor **1432** to validate credit card and debit card transactions, send a bill to customer **1450**, and report the transactions to publisher **1410**. Upon receipt of an affirmative response from electronic commerce vendor **1432**, rights clearinghouse **1430** issues a key or a permit for secure work **1415** to customer **1450**. Customer **1450** uses the key or permit to gain access to protected work **1413**. Rights clearinghouse **1430** updates a log or a database to report to publisher **1410** the aggregate sales numbers and the individual customer information. It is to be understood that publisher **1410**, rights clearinghouse **1430**, and electronic commerce vendor **1432** can perform the functions described above on either a single computer or a distributed network of computers. Furthermore, it is to be understood that the functions performed by rights clearinghouse **1430** and electronic commerce vendor **1432** can be performed by an entity other than publisher **1410**.

In another embodiment, customer **1450** can access secure work **1415** through content distributor, syndicator, or aggregator **1440**. The content distributor, syndicator, or aggregator **1440** will allow customer **1450** to browse metadata database **1422**. Metadata database **1422** includes, but is not limited to, a listing service, catalog service, or sales directory service. When customer **1450** demonstrates an interest in a work such as secure work **1415**, the content distributor, syndicator, or aggregator **1440** sends a request to content hosting **1420** and retrieves secure work **1415**. Content distributor, syndicator, or aggregator **1440** is also coupled to rights clearinghouse 1430 to coordinate, as described above, the payment by

customer **1450** for the rights associated with secure work **1415**. It is to be understood that publisher **1410** and content distributor, syndicator, or aggregator **1440** can perform the functions described above on either a single computer or a distributed network of computers. Furthermore, it is to be understood that the functions performed by content distributor, syndicator, or aggregator **1440** can be performed by an entity other than publisher **1410**.

The scenario illustrated in Figure **14** is a fragile system. Typically, each instance of the original digital work **1411** (i.e., protected work **1413** and secure work **1415**) is a separate resource. In addition, there may be several entities (i.e., publisher **1410**, DRM packaging software **1412**, secure wrapping and encryption **1414**, and content hosting **1420** and meta-data **1422** database) involved in the control and distribution of each instance of the original digital work **1411**. A link that customer **1450** finds while searching the Internet or browsing a catalog or peer-to-peer server is likely to be out-of-date. Similarly, content distributor, syndicator, or aggregator **1440** cannot guarantee the quality of a link or reference to secure work **1415** or protected work **1413**. Thus, there is a need for an apparatus, method, and system that will eliminate the fragility of the links and increase the durability of the system.

The scenario illustrated in Figure 14 is a fragile system for another reason as well, besides the absence of persistent links between the systems involved. This reason is the absence of a unique, unambiguous, universally-recognized identifier for the content itself. Typically, each instance of the original digital work **1411** (i.e., protected work **1413** and secure work **1415**) is a separate resource. In addition, there may be several entities (i.e., publisher **1410**, DRM packaging software **1412**, secure wrapping and encryption **1414**, and content hosting **1420** and meta-data **1422** database) involved in the control and distribution of each instance of the original digital work **1411**. If these entities cannot rely on a unique

identifier for the content, they cannot easily or reliably interoperate with each other – i.e., communicate with each other via a reliable method of referencing to the content. This is similar to the way that Universal Product Codes (a.k.a. bar codes) permit interoperability between many entities that must reference physical objects reliably, such as point-of-sale (POS) systems communicating with inventory control systems, inventory control systems communicating with "just-in-time" replenishment-ordering systems, replenishment-ordering systems communicating from a store to a distributor or manufacturer's ordering systems. But there is no corresponding identifier for objects of digital content except the DOI, and therefore there is a need for an apparatus, method, and system that will increase the durability of the system by eliminating the fragilities represented by the absence of an identifier to permit cross-system communication and interoperability.

Figure **14** also illustrates the integration of digital object identifiers (DOIs) into the traditional digital rights management scenario. At the time of publication of a work, publisher **1410** issues a unique DOI for that work, which is then registered with a DOI registration agency **1550**. The DOI is then used to unambiguously refer to the identified work in all manner of transactions throughout the rest of the system. For example, the content hosting provider **1420** would store and retrieve works based on their DOIs. In this way, when publisher **1410** wanted to update file **1415** hosted by the content hosting provider, it could transmit the updated file with instructions to replace the older version of the work identified by the same DOI.

In yet another example, rights clearinghouse **1430** that sold access permissions to customer **1450** uses the DOI to report sales figures for all of a publisher's various works back to the publisher on an ongoing basis. Currently, many rights clearinghouses report back sales

figures to publishers in a non-automatable, manual fashion, using bibliographic information such as, for example, title, author, and year of publication to attempt to unambiguously identify the works that have been sold. This requires publisher **1410** to manually transfer the sales information to their own systems, and is not guaranteed to make necessary distinctions between versions of the same work which are sold separately but share much of the same bibliographic information. Using each work's unique DOI to refer to that work assures all parties that they are referring to the same work, and allows for automated interoperability between disparate computer systems, such as the sales system of a rights clearinghouse and the financial systems of a publisher.

The same benefits of reliable, unambiguous identification and automated interoperability apply to all other communications channels in the DRM system illustrated in Figure **14**. For example, when customer **1450** purchases a key to access protected work **1413**, they can be assured that the key is correct and not one for another work by the same author, associated with a similar title, or in a different format or language. In yet another example, content distributor, syndicator or aggregator **1440** who wishes to present a number of available works by a single author to a community of customers **1450** can communicate with metadata database **1422** to look-up the DOIs of the relevant works, can transmit rights clearance requests using the DOI for each of the identified works to the rights clearinghouse **1430**, and can then download the works as needed from the content hosting service **1420** using the DOIs to request the appropriate works.

Multiple Resolution

Referring again to Figure 14, customer **1450** causes a request for DOI resolution to be made to the DOI system either by directly entering a DOI or by relying upon content

distributor, syndicator, or aggregator **1440** to enter the DOI, or by using end-user DRM software that can make a DOI request. The DOI request is sent to a DOI server and resolved to a piece of data, often a pointer in the form of a URL, associated with secure work **1411**. A DOI can resolve to one of many pieces of data, depending on the type of request made to the DOI system. Customer **1450** or content distributor, syndicator, or aggregator **1440** may choose to integrate the type of resolution request into the DOI request in the form of an enhanced DOI. Generally, the enhanced DOI will take the form "XXXX@10:1000/abc123defg, where XXXX is the argument or list of arguments to the DOI system. Publisher **1410** creates and registers types for the argument, XXXX, with the DOI server. For instance, a securely wrapped work may include, in the wrapper, an enhanced DOI, such as GET.RIGHTS@10.1000/abc123defg, that resolves to the location of the rights clearinghouse that can accept payment and unlock the content for authorized users. If the location of the rights clearinghouse moves, or if the publisher contracts with a different rights clearinghouse, the Handle System directory entry can be easily updated by publisher **1410**, and all existing DOI-based links will continue to work, even though they were created before the changes were instituted.

In yet another example, a customer who has received a piece of secured content who wishes to access an excerpt of the work before deciding whether to purchase the work, can make a request to the DOI system for the location of such an excerpt. The DOI system could respond with either the URL of a page containing an excerpt, or could point the user's DRM software to an access key that unlocks a small part of the secure file for a limited time and for no charge.

Digital Watermarking

Figure **15** illustrates the integration of a watermark into the digital rights management scenario shown in Figure **14**. Publisher **1544** must register work **1545** with DOI registration agency **1550** to receive a unique DOI to assign to the work. Registration agency **1550** stores metadata that describes work **1545** in DOI lookup database **1552**. In addition, a number of services are registered, associated with the unique DOI, and registered by registration agency **1550** in DOI system **1530**. Figure **15** depicts publisher **1544** as coupled to registration agency **1550** by a direct communications connection. It is to be understood that communications between publisher **1544**, registration agency **1550**, DOI lookup database **1552**, and DOI system **1530** can take place over a network such as Internet **1520**.

Once work **1545** is registered with DOI registration agency **1550**, publisher **1544** forwards work **1545** to watermarking and tagging system **1542**. Watermarking and tagging system **1542** embeds a watermark in a digital work by adding extra information to the digital work in such a manner that the extra information does not degrade the quality of the digital work. Numerous acceptable methods exist in the prior art for applying a watermark to a digital image, movie, or audio file, however, only one watermarking method will be detailed in this disclosure. The novel aspect disclosed herein pertains to the use of the DOI as part of the information included in the digital watermark. Since a DOI is resolvable or actionable, anyone who can extract the watermark can use the DOI to initiate contact with the current holder of the property rights associated with work **1545** and can access the most up-to-date locations for various registered services associated with the work. For example, if a digital image is watermarked with the DOI for the digital image, a user who encounters the digital image on a website can extract the DOI and automatically place a request for the rights to

reuse the digital image. The user may also retrieve the most up-to-date information about the photographer and the subject of the photograph, and could be offered a high-resolution version of the same photo for use in their print publications. It is to be understood that publisher **1544** and watermarking and tagging system **1542** can perform the functions described above on either a single computer or a distributed network of computers. Furthermore, it is to be understood that the functions performed by watermarking and tagging system **1542** can be performed by an entity other than publisher **1544**.

One prior art method of watermarking an image file is least significant bit watermarking. A standard image file represents an image as a grid of picture elements or pixels, wherein each pixel corresponds to a region of the image. A high-quality image may require 90,000 pixels to represent each square inch of the image. A number is assigned to each pixel that indicates the color and brightness that best describes region of the image that corresponds to the pixel. An 8-bit grayscale image, for example, assigns each pixel a number between 0 and 255 to indicate the brightness of the region of the image, where the value 0 represents black, the value 255 represents white, and the value 127 represents a medium shade of gray. Since the range 0 to 255 can be represented with 8 bits in base 2 or binary, each pixel value requires 8 bits of storage. For example, a pixel value of decimal 155 after conversion to base 2 notation is "10011011" (i.e., 10011011 (base 2) = 1*128 + 0*64 + 0*32 + 1*16 + 1*8 + 0*4 + 1*2 + 1*1 = 155 (base 10 or decimal). Thus, the image can be represented by a long series of binary digits or bits that can only be either 0 or 1.

In the example shown above, since the rightmost digit of "10011011" is multiplied by the lowest power of the base, the value of the rightmost digit has the least impact on the value of the number. Thus, the rightmost digit is called the "least significant digit" or for binary

numbers the "least significant bit". Altering the least significant bit of every pixel in an image file of sufficient depth (i.e., with a large enough range of possible values) will, therefore, rarely result in visible degradation of the image.

Least significant bit watermarking encodes a message as a string of bits into an image by replacing the least significant bit of each pixel value in a selected range of pixel values. This method of digital watermarking is not typically detectable to the human eye because the alteration at most change the value of each pixel by 1 unit. Even for a low-quality 8-bit grayscale image, a 1 unit change in shading is not generally detectable to the human eye. If a viewer of the image expects a watermark and knows how to analyze the image, the user can extract the encoded message.

Least significant bit watermarking is known to be a "fragile watermark" because it can easily be removed from the file either intentionally (e.g. by replacing the least significant bits of every pixel with zeros), or unintentionally (e.g. by compressing the image using a lossy compressor, or by cropping, or zooming the image). There are other publicly available, more robust methods for encoding a watermark in a digital file, which are well-known to those trained in the art.

Figures **16A** is a flow diagram of an embodiment of the watermarking process shown in Figure **15** that results in a user opening a protected digital work. The process shown in Figure **16A** begins at step **1610** by a publisher creating a digital work. Once the work is created, the publisher contacts a registration authority to assign a unique DOI to the work at step **1612**. At step **1614**, the publisher establishes and registers DOI service bindings to the work. Finally, the publisher registers and stores metadata with the registration agency at step **1616**. The metadata includes, but is not limited to, bibliographic data, sensory fingerprint

data, and checksum data. At step **1618**, the publisher uses software to wrap and encrypt the work using the DOI as the watermark. At step **1620**, a user encounters the wrapped and encrypted work and opens the content using DRM software that can extract the DOI-based watermark and gain access to the content.

Figure **16B** is a flow diagram of an embodiment of the watermarking process shown in Figure **15** that results in a user accessing a hacked digital work. The process shown in Figure **16B** begins at step **1630** by a publisher creating a digital work. Once the work is created, the publisher contacts a registration authority to assign a unique DOI to the work at step **1632**. At step **1634**, the publisher establishes and registers DOI service bindings to the work. Finally, the publisher registers and stores metadata with the registration agency at step **1636**. The metadata includes, but is not limited to, bibliographic data, sensory fingerprint data, and checksum data. At step **1638**, the publisher uses software to wrap and encrypt the work using the DOI as the watermark. At step **1640**, a user encounters the wrapped and encrypted work after the work has been hacked or corrupted and subsequently redistributed. Thus, the DOI watermark is invalid or not retrievable. At step **1644**, relegitimization software analyzes the hacked or corrupted work and computes a sensory fingerprint for the work. At step **1646**, the relegitimization software contacts the DOI system to look-up the works DOI based on the metadata, allowing the user to open the content using DRM software that can use the DOI to gain access to the content and to other services associated with the work.

Figure **16C** is a flow diagram of an embodiment of the watermarking process shown in Figure **15** that results in a user accessing an informally distributed digital work. The process shown in Figure **16C** begins at step **1650** by a publisher publishing a work using a traditional means such as distribution of a print version of a journal that contains the work.

Following traditional publication of the work, the flow splits into two paths. One path begins at step **1658** when someone creates a digital representation of the work and, at step **1660**, distributes the digital work through some informal means. Informal distribution of the work, for example, includes posting a portable data format (PDF) version of the work on a public web site. The other path begins at step **1652** when the publisher contacts a registration authority to assign a unique DOI to the work. At step **1654**, the publisher establishes and registers DOI service bindings to the work. Finally, the publisher registers and stores metadata with the registration agency at step **1656**. Step **1662** unites the split flow by using the relegitimization software to attach the unique DOI from step **1652** with the informally distributed version of the work from step **1660**. A user can now open the informally distributed PDF version of the work using DRM software that can use the DOI to gain access to the content and to other services associated with the work.

Validation

Figure **17** illustrates the integration of a validation architecture into the digital rights management scenario shown in Figure **14**. Validating computer **1730** retrieves a digital work such as protected work **1413** via a network such as Internet **1720**. The digital work can originate from an electronic transfer source including electronic mail server **1710**, web server **1712**, or another user **1714** computer. Alternatively, validating computer **1730** can receive the digital work by reading the file directly from a physical medium such as a removable disk, memory storage card, or the like.

Software on validating computer **1730** determines the DOI for the work embodied in the file just retrieved. This could be accomplished by any of several methods. First, the DOI could have been retrieved with the file when it was downloaded and stored in memory for

validating computer **1730**. Second, the DOI could be extracted from a watermark placed in the file by the publisher of the file. Third, the DOI for the work could be retrieved by a look-up using DOI Search Engine **1740**, using known bibliographic information (title, author, date of publication, etc.), or other metadata for the file (song length, sensory "fingerprint" of image or song file, checksum or hash result for an executable file, etc.).

Software on validating computer **1730** then issues a query to DOI system **1742** to request validation credentials for the work identified by the given DOI. DOI system **1742** either responds with the file's credentials or responds with a pointer (e.g., URL) to the location of those credentials in validation data repository **1744**. The credentials should either be of a known type, or should provide information on how the validation process should proceed.

Validation software executing on validating computer **1730** then performs an analysis of the file originally retrieved to determine whether it matches the validation credentials retrieved. Generally, this involves performing a series of calculations using the original file as an input such that the result of these calculations is of a fixed, short length, and is likely to be different if the file has been modified since it was first published. In this way the user can determine whether the file is an authentic copy of the originally published document. If the file is determined to be an invalid or corrupted version of the work the software can use the discovered DOI to look-up sales outlets and the user can be immediately offered the chance to purchase or acquire a valid copy of the work.

Many straightforward hash algorithms with a very low probability of generating the same output for different inputs exist, such as MD-5 and SHA. In the case of an image, sound, movie or other multimedia file, it may be desirable to use a method of validation that

detects differences between files perceptible to humans. In this way, if a song is copied from a CD by a user, and converted to another file format, the algorithm might still, by using perceptual criteria, determine that the song had not been modified since publication, and validate the work. One such perceptual algorithm is being deployed by Napster today to track which songs being traded on its file-sharing network. More detailed information on Napster's perceptual algorithm can be found at "www.relatable.com/news/pressreleases/010420.release.html".

Although the embodiments disclosed herein describe a fully functioning apparatus, method, and system for accessing a digitized work of authorship protected by a digital rights management system, the reader should understand that other equivalent embodiments exist. Since numerous modifications and variations will occur to those who review this disclosure, the apparatus, method, and system for accessing a digitized work of authorship protected by a digital rights management system is not limited to the exact construction and operation illustrated and disclosed herein. Accordingly, this disclosure intends all suitable modifications and equivalents to fall within the scope of the claims.

Multiple Resolution Menu Facility (MRMF)

Figures 18 and 19 illustrate a schematic diagram of one non-limiting example embodiment of an interactive interface multiple resolution menu facility (MRMF). In Figure 18, a DOI may be provided in any number of manners to a user. In one example, a DOI is embedded in a Portable Document Format (PDF) 1801 and viewed in an Electronic Book (e-book) reader 1805 such as Adobe's Acrobat, Adobe's E-book Reader, Microsoft's E-book Reader, and/or the like. The DOI 1802 (e.g., in Figure 18, the DOI is the highlighted text "Click here," which may actually embed a DOI number and/or reference as metadata that is

presented to the user as the highlighted text) may be engaged by a user selection facility such as but not limited to a pointing cursor 1803. By selecting the DOI 1802, an interactive interface menu is generated 1804. The MRMF may be implemented as a module using a number of standard development tools such as, but not limited to: C, C++, Java, Javascript, Objective-C, Perl, Python, and/or the like. The MRMF may be integrated into the DRMS controller's user interface. In an alternative embodiment, the MRMF may be implemented as a plug-in for a viewing application such as, but not limited to: Adobe's Acrobat, Adobe's E-book Reader, Microsoft's E-book Reader, Microsoft Explorer, Microsoft Internet Explorer, Netscape Navigator, and/or the like. The MRMF module logic generally is engaged upon being loaded by a viewing application and more specifically when the user selects a DOI 1802.

Upon engaging the DOI 1802 with a cursor 1803, the MRMF obtains a list of multiple resolution options for display and further selection. The list may be generated by reading the DOI embedded into the document and resolving the DOI with a DOI resolution server. In one example, an enhanced DOI grammar may be employed to poll all multiple resolution options from the DOI resolution server, e.g., poll.allResolutions@DOI, poll.allAcmeIncResolutions@DOI. The DOI resolution server will then return a list of all and/or some resolution options stored within the record for the particular DOI from the DOI resolution server. Upon obtaining this list from the DOI resolution server, the MRMF will parse the results if needed and generate a menu list corresponding to the resolution options returned from the DOI resolution server 1804.

Upon displaying the list of options to a user 1804, the user may continue and select any of the displayed options in the option expanded MRMF. Thereafter the user may select

one of the displayed multiple resolution options presented in the option expanded MRMF, e.g., by clicking a mouse button on a mouse to engage the cursor's selection engagement mechanism 1806, 1807. It should be noted that a menu hierarchy 1804, 1806, 1807 may be constructed by parsing the results of the DOI resolution server poll, wherein the results obtained have common headers; e.g., the DOI resolution server may return poll results in the form of enhanced DOIs such as BuyBook.Print@DOI, BuyBook.AdobeEBookReader@DOI, and BuyBook.MicrosoftReader@DOI, which may all be parsed to build a menu with a root of "BuyBook" and sub-menus "Print," "AdobeEBook," and "MicrosoftReader." It should be further noted that the poll results from the DOI resolution server may themselves be DOIs, wherein the MRMF may then further recursively poll based on such DOI poll results thereby building up a larger menu of multiple resolution options for a user. By engaging one of the options, the MRMF initiates a specific DOI resolution to the multiple resolution option that was selected by the user. For example, by selecting an option to "Buy Book" 1804, "Print" 1806, and "Amazon.com" 1807, 1803, the MRMF will resolve an option to a web page on Amazon.com where a printed version (and/or any other specified versions) of the information represented by the DOI may be purchased.

In Figure 19, in one example embodiment, the MRMF further presents the user with an "E-mail a Friend" option 1805. If the user engages the "E-mail a Friend" option 1805, the MRMF will generate a signal to generate a new E-mail to the operating system. The MRMF may generate a signal by employing any number of system APIs such as those in win32 development libraries, Lotus Notes APIs, Microsoft Outlook Express APIs, Microsoft Outlook Express APIs, and/or the like. The MRMF makes a call through the proper API requesting (the launch and instantiation of an E-mail application if necessary and) the

instantiation of a new E-mail window 1908. The MRMF will instruct an instantiated E-mail application via its API to create a new E-mail message with a copy of the DOI 1906 from which the user made a selection. Thereafter, the user may address the E-mail to a his/her friend's E-mail address 1907 (or to any other recipients, e.g., a distribution list) along with any desired comments 1909, 1910 and send the DOI via E-mail for another user to interact with the DOI.

In one example embodiment, the new E-mail message is automatically generated and an MRMF plug-in is attached to the E-mail message with instructions to install the plug-in and thus enable MRMF facilities where they were absent. In another embodiment, the DOI is embedded as a hyperlink which allows a designated server to provide the MRMF functionality, e.g., http://www.doiResolutionReRoutingServer.com/poll.allResolutions@DOI. In yet another embodiment, the MRMF functionality is provided by a server to the user's device by downloading a module from a designated server, e.g., as Javascript, as a window engaged in communications with a server, and/or the like.

We claim:

1. A method of accessing a digital work from a computer comprising:

selecting an unique, persistent, and universal name identifier for the digital work;

associating at least one usage right with the digital work to create a protected digital work;

storing the protected digital work and the unique, persistent, and universal name identifier in a directory that maintains universal resource names and locations for information associated with the universal resource names;

issuing a query from the computer to the directory to generate a result set that includes the unique, persistent, and universal name identifier; and

retrieving from the directory the protected digital work with the unique, persistent, and universal name identifier.

2. The method of claim 1, wherein the unique, persistent, and universal name identifier is a digital object identifier (DOI).

3. The method of claim 1, wherein said at least one usage right allows a user to perform an action on the digital work with the computer.

4. The method of claim 3, wherein the action is to display the digital work.

5. The method of claim 3, wherein the action is to copy the digital work.

6. The method of claim 3, wherein the action is to forward the digital work to another computer.

7. The method of claim 3, wherein the action is to print the digital work.

8. The method of claim 1, wherein after the associating, the method further comprises:

encrypting the protected digital work.

9. The method of claim 1, wherein after the associating, the method further comprises:

wrapping the protected digital work by encasing the digital work in a secure container.

10. The method of claim 9, wherein the secure container includes a digital watermark.

11. The method of claim 10, wherein the digital watermark includes the unique, persistent, and universal name identifier.

12. The method of claim 1, further comprising:

storing metadata that describes the protected digital work and the unique, persistent, and universal name identifier.

13. The method of claim 12, wherein the query includes the metadata.

14. The method of claim 1, wherein the computer is a mobile device.

15. The method of claim 1, wherein the directory is a catalog that indexes digital works of authorship.

16. The method of claim 1, wherein the directory is part of a peer-to-peer network.

17. The method of claim 1, wherein a content distributor, a content syndicator, or a content aggregator issues the query on behalf of the computer.

18. A method of accessing a digital work associated with a unique, persistent, and universal name identifier, a protected digital work received from another computer, the protected digital work including the digital work and at least one usage right associated with the digital work, comprising:

issuing a query from the computer to a directory, that maintains universal resource names and locations for information associated with the universal resource names, to generate a result set that includes the unique, persistent, and universal name identifier;

establishing a connection to a rights clearinghouse to validate the protected digital work;

receiving a key in response to a successful financial transaction; and

accessing the digital work by performing an action allowed by said at least one usage right on the protected digital work with the key.

19. The method of claim 18, wherein the unique, persistent, and universal name identifier is a digital object identifier (DOI).

20. The method of claim 18, wherein the rights clearinghouse updates a reporting log.

21. The method of claim 20, wherein the reporting log includes sales data.

22. The method of claim 20, wherein the reporting log includes customer data.

23. The method of claim 20, wherein the reporting log is in an electronic form and the rights clearinghouse periodically sends reporting log to a publisher of the digital work.

24. A method of accessing a digital work associated with a unique, persistent, and universal name identifier, comprising:

issuing a query from the computer to a directory, that maintains universal resource names and locations for information associated with the universal resource names, to obtain a list of reference options;

receiving query results from the directory;

building a menu based on the query results; and

displaying the menu, wherein the menu may be engaged by a user to select and access a specific reference option.

25. The method of claim 24, further comprising displaying a menu option to send the unique, persistent, and universal name identifier via E-mail, wherein selecting the send E-mail option instantiated a new E-mail with the universal resource name embedded within the new E-mail.

26. A system for accessing a digital work from a computer comprising:

means to select an unique, persistent, and universal name identifier for the digital work;

means to associate at least one usage right with the digital work to create a protected digital work;

means to store the protected digital work and the unique, persistent, and universal name identifier in a directory that maintains universal resource names and locations for information associated with the universal resource names;

means to issue a query from the computer to the directory to generate a result set that includes the unique, persistent, and universal name identifier; and

means to retrieve from the directory the protected digital work with the unique, persistent, and universal name identifier.

27. The system of claim 26, wherein the unique, persistent, and universal name identifier is a digital object identifier (DOI).

28. The system of claim 26, wherein said at least one usage right allows a user to perform an action on the digital work with the computer.

29. The system of claim 28, wherein the action is to display the digital work.

30. The system of claim 28, wherein the action is to copy the digital work.

31. The system of claim 28, wherein the action is to forward the digital work to another computer.

32. The system of claim 28, wherein the action is to print the digital work.

33. The system of claim 26, wherein after the associating, the system further comprises:

means to encrypt the protected digital work.

34. The system of claim 26, wherein after the associating, the system further comprises:

means to wrap the protected digital work by encasing the digital work in a secure container.

35. The system of claim 34, wherein the secure container includes a digital watermark.

36. The system of claim 35, wherein the digital watermark includes the unique, persistent, and universal name identifier.

37. The system of claim 26, further comprising:

means to store metadata that describes the protected digital work and the unique, persistent, and universal name identifier.

38. The system of claim 37, wherein the query includes the metadata.

39. The system of claim 26, wherein the computer is a mobile device.

40. The system of claim 26, wherein the directory is a catalog that indexes digital works of authorship.

41. The system of claim 26, wherein the directory is part of a peer-to-peer network.

42. The system of claim 26, wherein a content distributor, a content syndicator, or a content aggregator issues the query on behalf of the computer.

43. A system for accessing a digital work associated with a unique, persistent, and universal name identifier, a protected digital work received from another computer, the protected digital work including the digital work and at least one usage right associated with the

digital work, comprising:

means to issue a query from the computer to a directory, that maintains universal resource names and locations for information associated with the universal resource names, to generate a result set that includes the unique, persistent, and universal name identifier;

means to establish a connection to a rights clearinghouse to validate the protected digital work;

means to receive a key in response to a successful financial transaction; and

means to access the digital work by performing an action allowed by said at least one usage right on the protected digital work with the key.

44. The system of claim 43, wherein the unique, persistent, and universal name identifier is a digital object identifier (DOI).

45. The system of claim 43, wherein the rights clearinghouse updates a reporting log.

46. The system of claim 45, wherein the reporting log includes sales data.

47. The system of claim 45, wherein the reporting log includes customer data.

48. The system of claim 45, wherein the reporting log is in an electronic form and the rights clearinghouse periodically sends reporting log to a publisher of the digital work.

49. A system for accessing a digital work associated with a unique, persistent, and

universal name identifier, comprising:

means to issue a query from the computer to a directory, that maintains universal resource names and locations for information associated with the universal resource names, to obtain a list of reference options;

means to receive query results from the directory;

means to build a menu based on the query results; and

means to display the menu, wherein the menu may be engaged by a user to select and access a specific reference option.

50. The system of claim 49, further comprising displaying a menu option to send the unique, persistent, and universal name identifier via E-mail, wherein selecting the send E-mail option instantiated a new E-mail with the universal resource name embedded within the new E-mail.

51. A program stored on a medium readable by a processor, the program, comprising:

a module to select an unique, persistent, and universal name identifier for the digital work;

a module to associate at least one usage right with the digital work to create a protected digital work;

a module to store the protected digital work and the unique, persistent, and universal name identifier in a directory that maintains universal resource names and locations for information associated with the universal resource names;

a module to issue a query from the computer to the directory to generate a result

set that includes the unique, persistent, and universal name identifier; and

a module to retrieve from the directory the protected digital work with the unique, persistent, and universal name identifier.

52. The medium of claim 51, wherein the unique, persistent, and universal name identifier is a digital object identifier (DOI).

53. The medium of claim 51, wherein said at least one usage right allows a user to perform an action on the digital work with the computer.

54. The medium of claim 53, wherein the action is to display the digital work.

55. The medium of claim 53, wherein the action is to copy the digital work.

56. The medium of claim 53, wherein the action is to forward the digital work to another computer.

57. The medium of claim 53, wherein the action is to print the digital work.

58. The medium of claim 51, wherein after the associating, the medium further comprises:

a module to encrypt the protected digital work.

59. The medium of claim 51, wherein after the associating, the medium further comprises:

a module to wrap the protected digital work by encasing the digital work in a secure container.

60. The medium of claim 59, wherein the secure container includes a digital watermark.

61. The medium of claim 60, wherein the digital watermark includes the unique, persistent, and universal name identifier.

62. The medium of claim 51, further comprising:

a module to store metadata that describes the protected digital work and the unique, persistent, and universal name identifier.

63. The medium of claim 62, wherein the query includes the metadata.

64. The medium of claim 51, wherein the computer is a mobile device.

65. The medium of claim 51, wherein the directory is a catalog that indexes digital works of authorship.

66. The medium of claim 51, wherein the directory is part of a peer-to-peer network.

67. The medium of claim 51, wherein a content distributor, a content syndicator, or a content aggregator issues the query on behalf of the computer.

68. A program stored on a medium readable by a processor for accessing a digital work associated with a unique, persistent, and universal name identifier, a protected digital work received from another computer, the protected digital work including the digital work and at least one usage right associated with the digital work, the program, comprising:

a module to issue a query from the computer to a directory, that maintains universal resource names and locations for information associated with the universal resource names, to generate a result set that includes the unique, persistent, and universal name identifier;

a module to establish a connection to a rights clearinghouse to validate the protected digital work;

a module to receive a key in response to a successful financial transaction; and

a module to access the digital work by performing an action allowed by said at least one usage right on the protected digital work with the key.

69. The medium of claim 68, wherein the unique, persistent, and universal name identifier is a digital object identifier (DOI).

70. The medium of claim 68, wherein the rights clearinghouse updates a reporting log.

71. The medium of claim 70, wherein the reporting log includes sales data.

72. The medium of claim 70, wherein the reporting log includes customer data.

73. The medium of claim 70, wherein the reporting log is in an electronic form and the rights clearinghouse periodically sends reporting log to a publisher of the digital work.

74. A program stored on a medium readable by a processor for accessing a digital work associated with a unique, persistent, and universal name identifier, the program, comprising:

a module to issue a query from the computer to a directory, that maintains universal resource names and locations for information associated with the universal resource names, to obtain a list of reference options;

a module to receive query results from the directory;

a module to build a menu based on the query results; and

a module to display the menu, wherein the menu may be engaged by a user to select and access a specific reference option.

75. The medium of claim 74, further comprising displaying a menu option to send the unique, persistent, and universal name identifier via E-mail, wherein selecting the send E-mail option instantiated a new E-mail with the universal resource name embedded within the new E-mail.

76. An apparatus, comprising:

a processor;

a memory, communicatively connected to the processor,

a program, stored in the memory, including,,

a module to select an unique, persistent, and universal name identifier for the digital work;

a module to associate at least one usage right with the digital work to create a protected digital work;

a module to store the protected digital work and the unique, persistent, and universal name identifier in a directory that maintains universal resource names and locations for information associated with the universal resource names;

a module to issue a query from the computer to the directory to generate a result set that includes the unique, persistent, and universal name identifier; and

a module to retrieve from the directory the protected digital work with the unique, persistent, and universal name identifier.

77. The apparatus of claim 76, wherein the unique, persistent, and universal name identifier is a digital object identifier (DOI).

78. The apparatus of claim 76, wherein said at least one usage right allows a user to perform an action on the digital work with the computer.

79. The apparatus of claim 78, wherein the action is to display the digital work.

80. The apparatus of claim 78, wherein the action is to copy the digital work.

81. The apparatus of claim 78, wherein the action is to forward the digital work to another computer.

82. The apparatus of claim 78, wherein the action is to print the digital work.

83. The apparatus of claim 76, wherein after the associating, the apparatus further comprises:

a module to encrypt the protected digital work.

84. The apparatus of claim 76, wherein after the associating, the apparatus further comprises:

a module to wrap the protected digital work by encasing the digital work in a secure container.

85. The apparatus of claim 84, wherein the secure container includes a digital watermark.

86. The apparatus of claim 85, wherein the digital watermark includes the unique, persistent, and universal name identifier.

87. The apparatus of claim 76, further comprising:

a module to store metadata that describes the protected digital work and the unique, persistent, and universal name identifier.

88. The apparatus of claim 87, wherein the query includes the metadata.

89. The apparatus of claim 76, wherein the computer is a mobile device.

90. The apparatus of claim 76, wherein the directory is a catalog that indexes digital works of authorship.

91. The apparatus of claim 76, wherein the directory is part of a peer-to-peer network.

92. The apparatus of claim 76, wherein a content distributor, a content syndicator, or a content aggregator issues the query on behalf of the computer.

93. An apparatus, comprising:

a processor;

a memory, communicatively connected to the processor,

a program, stored in the memory, the program for accessing a digital work associated with a unique, persistent, and universal name identifier, a protected digital work received from another computer, the protected digital work including the digital work and at least one usage right associated with the digital work, the program, including,

a module to issue a query from the computer to a directory, that maintains universal resource names and locations for information associated with the universal resource names, to generate a result set that includes the unique, persistent, and universal name identifier;

a module to establish a connection to a rights clearinghouse to validate the protected digital work;

a module to receive a key in response to a successful financial transaction; and

a module to access the digital work by performing an action allowed by said at least one usage right on the protected digital work with the key.

94. The apparatus of claim 93, wherein the unique, persistent, and universal name identifier is a digital object identifier (DOI).

95. The apparatus of claim 93, wherein the rights clearinghouse updates a reporting log.

96. The apparatus of claim 95, wherein the reporting log includes sales data.

97. The apparatus of claim 95, wherein the reporting log includes customer data.

98. The apparatus of claim 95, wherein the reporting log is in an electronic form and the rights clearinghouse periodically sends reporting log to a publisher of the digital work.

99. An apparatus, comprising:

a processor;

a memory, communicatively connected to the processor,

a program, stored in the memory, the program for accessing a digital work associated with a unique, persistent, and universal name identifier, the program, including,,

a module to issue a query from the computer to a directory, that maintains universal resource names and locations for information associated with the universal resource names, to obtain a list of reference options;

a module to receive query results from the directory;

a module to build a menu based on the query results; and

a module to display the menu, wherein the menu may be engaged by a user to select and access a specific reference option.

100. The apparatus of claim 99, further comprising displaying a menu option to send the unique, persistent, and universal name identifier via E-mail, wherein selecting the send E-mail option instantiated a new E-mail with the universal resource name embedded within the new E-mail.

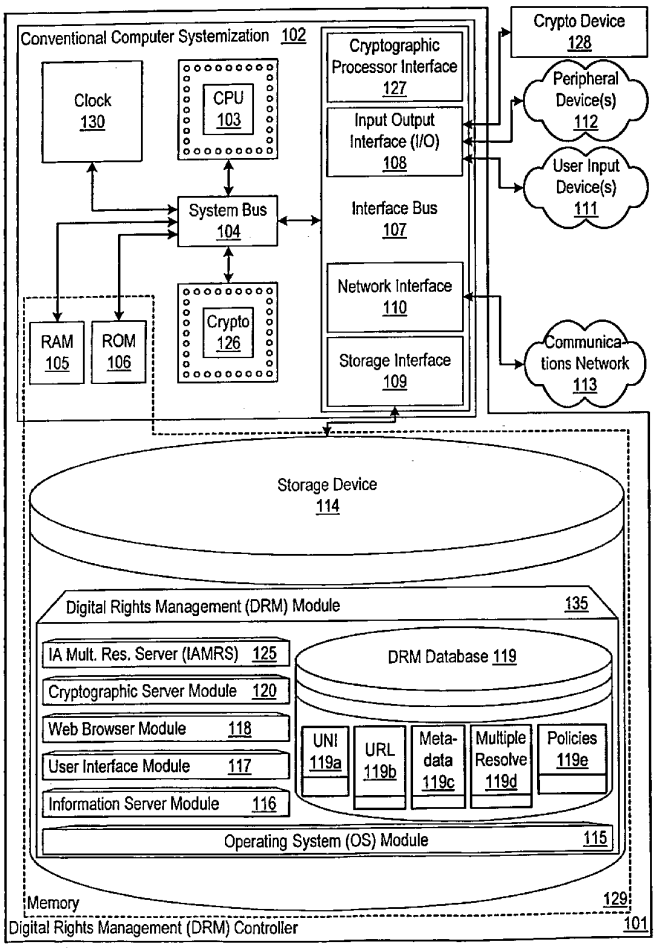

Conventional Computer Systemization 102
Clock 130
CPU 103
System Bus 104
RAM 105
ROM 106
Crypto 126
Cryptographic Processor Interface 127
Input Output Interface (I/O) 108
Interface Bus 107
Network Interface 110
Storage Interface 109
Crypto Device 128
Peripheral Device(s) 112
User Input Device(s) 111
Communications Network 113
Storage Device 114
Digital Rights Management (DRM) Module 135
IA Mult. Res. Server (IAMRS) 125
Cryptographic Server Module 120
Web Browser Module 118
User Interface Module 117
Information Server Module 116
DRM Database 119
UNI 119a
URL 119b
Meta-data 119c
Multiple Resolve 119d
Policies 119e
Operating System (OS) Module 115
Memory 129
Digital Rights Management (DRM) Controller 101

Figure 1

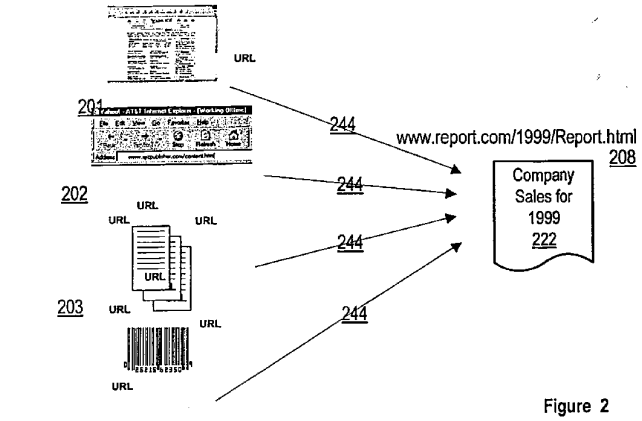


Figure 2

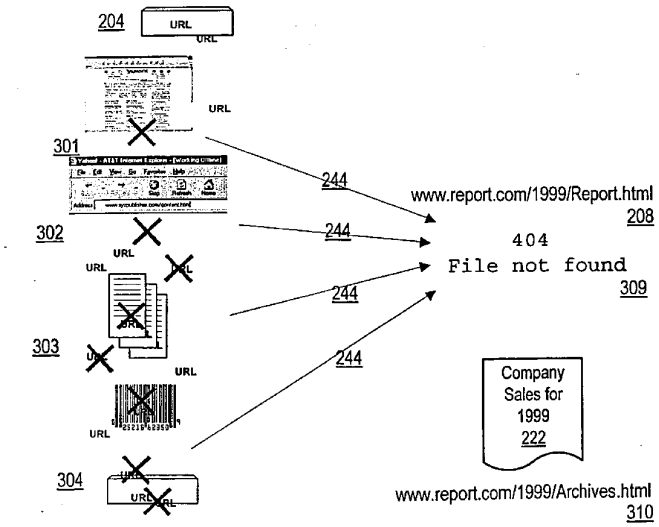


Figure 3

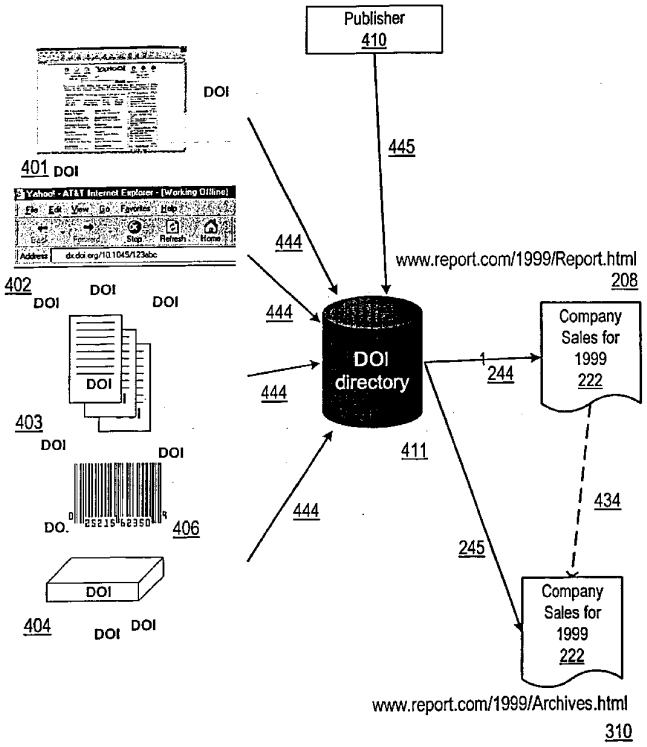

Publisher
410
DOI
401 DOI
445
444
www.report.com/1999/Report.html
208
402
DOI
DOI
DOI
444
DOI
directory
Company
Sales for
1999
222
244
DOI
403
DOI
DOI
411
434
444
DO.
406
245
DOI
Company
Sales for
1999
222
404
DOI
DOI
www.report.com/1999/Archives.html
310

Figure 4

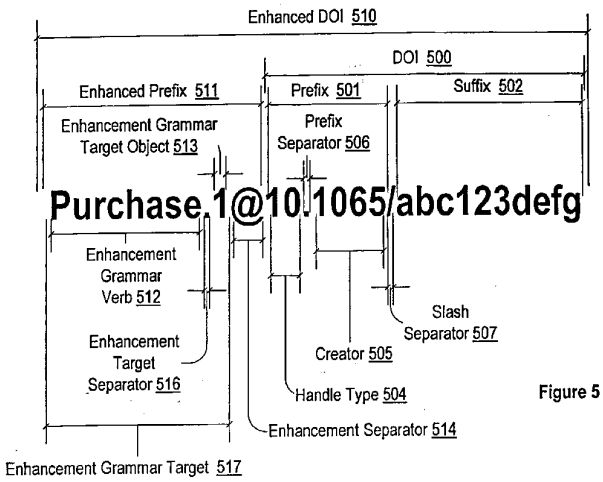


Figure 5

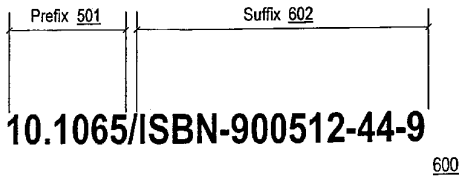


Figure 6

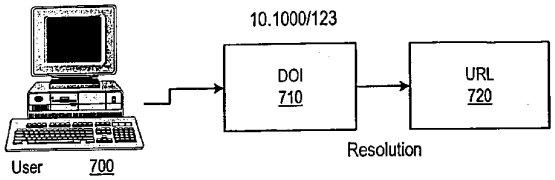


Figure 7

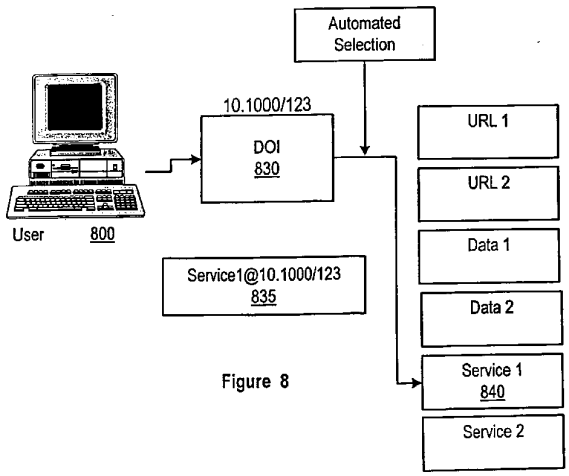


Figure 8

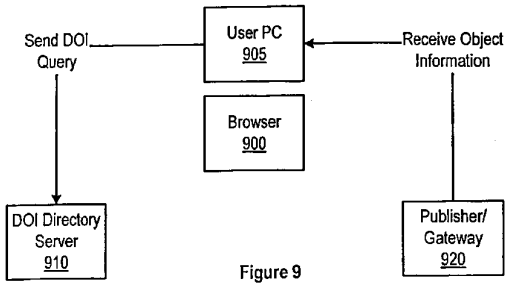


Figure 9

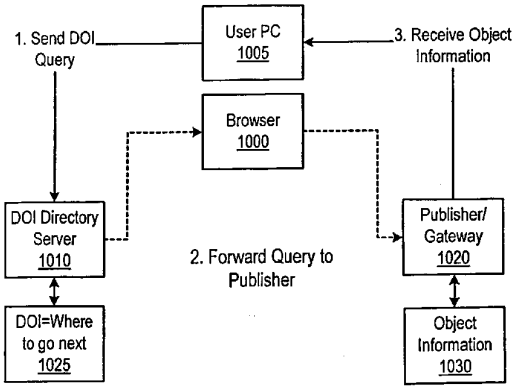


Figure 10

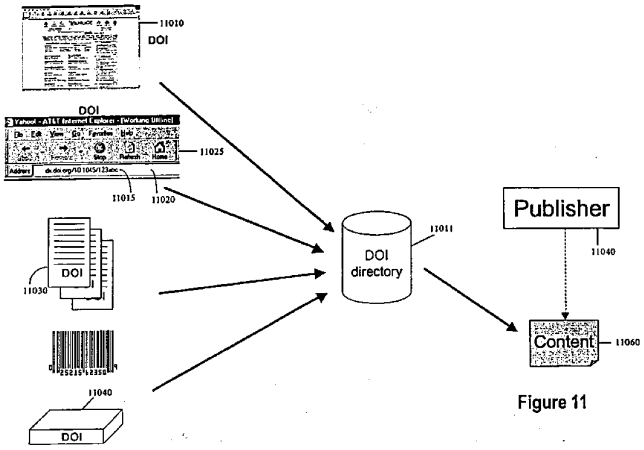


Figure 11

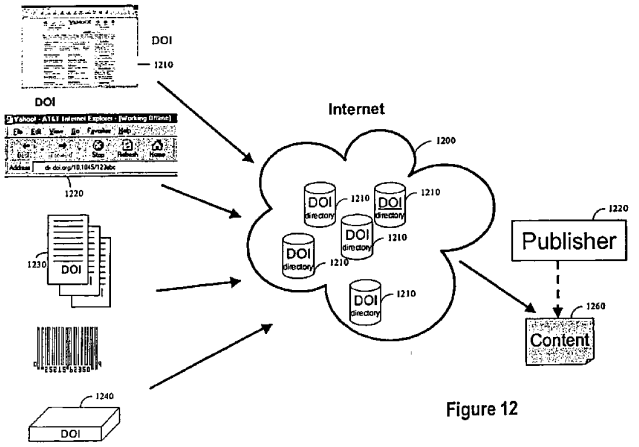


Figure 12

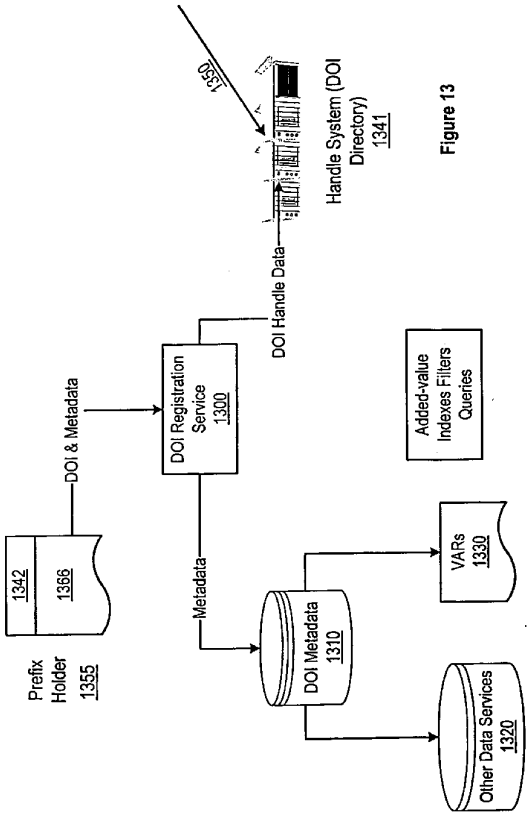

1350
Handle System (DOI Directory) 1341
DOI Handle Data
DOI Registration Service 1300
DOI & Metadata
Added-value Indexes Filters Queries
1342
1366
Prefix Holder 1355
Metadata
DOI Metadata 1310
VARs 1330
Other Data Services 1320

Figure 13

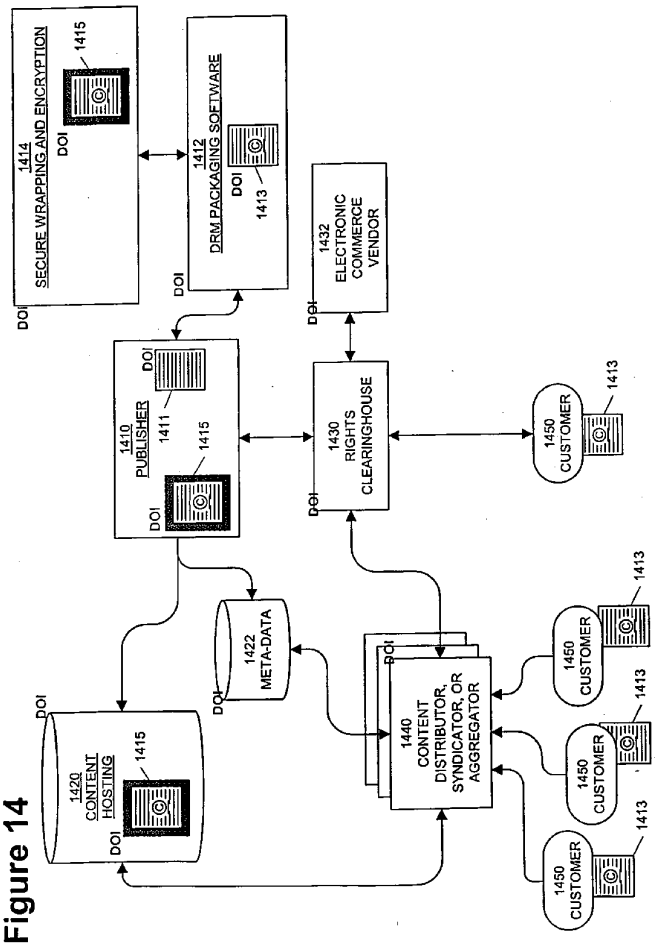

1414
SECURE WRAPPING AND ENCRYPTION
1415
DOI
1412
DRM PACKAGING SOFTWARE
DOI
1413
1432
ELECTRONIC
COMMERCE
VENDOR
1410
PUBLISHER
1411
1430
RIGHTS
CLEARINGHOUSE
1450
CUSTOMER
1422
META-DATA
1420
CONTENT
HOSTING
1440
CONTENT
DISTRIBUTOR,
SYNDICATOR, OR
AGGREGATOR

Figure 14

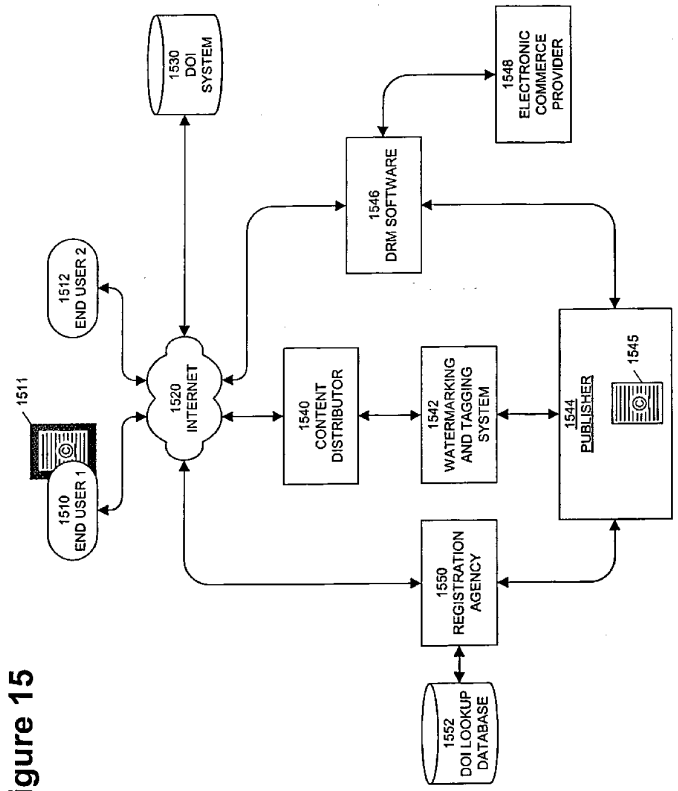

1530 DOI SYSTEM
1548 ELECTRONIC COMMERCE PROVIDER
1546 DRM SOFTWARE
1512 END USER 2
1511
1520 INTERNET
1540 CONTENT DISTRIBUTOR
1542 WATERMARKING AND TAGGING SYSTEM
1544 PUBLISHER
1545
1510 END USER 1
1550 REGISTRATION AGENCY
1552 DOI LOOKUP DATABASE

Figure 15

Figure 16A

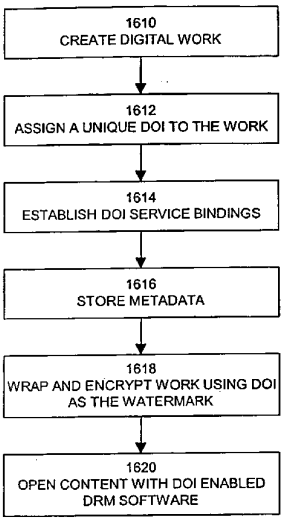

1610
CREATE DIGITAL WORK
1612
ASSIGN A UNIQUE DOI TO THE WORK
1614
ESTABLISH DOI SERVICE BINDINGS
1616
STORE METADATA
1618
WRAP AND ENCRYPT WORK USING DOI AS THE WATERMARK
1620
OPEN CONTENT WITH DOI ENABLED DRM SOFTWARE

Figure 16B

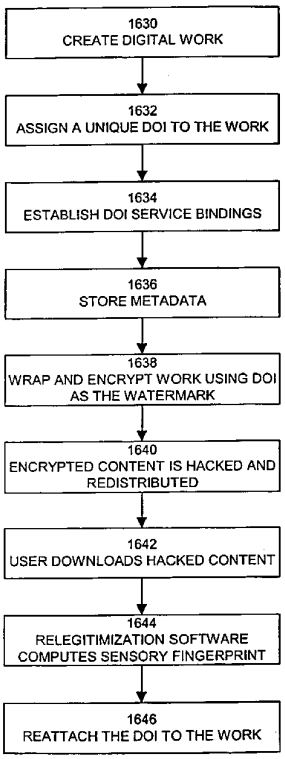
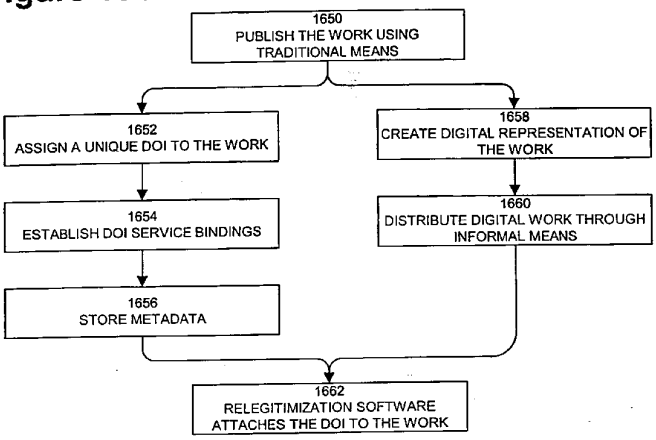

1630
CREATE DIGITAL WORK
1632
ASSIGN A UNIQUE DOI TO THE WORK
1634
ESTABLISH DOI SERVICE BINDINGS
1636
STORE METADATA
1638
WRAP AND ENCRYPT WORK USING DOI AS THE WATERMARK
1640
ENCRYPTED CONTENT IS HACKED AND REDISTRIBUTED
1642
USER DOWNLOADS HACKED CONTENT
1644
RELEGITIMIZATION SOFTWARE COMPUTES SENSORY FINGERPRINT
1646
REATTACH THE DOI TO THE WORK

Figure 16C


1650
PUBLISH THE WORK USING TRADITIONAL MEANS
1652
ASSIGN A UNIQUE DOI TO THE WORK
1654
ESTABLISH DOI SERVICE BINDINGS
1656
STORE METADATA
1658
CREATE DIGITAL REPRESENTATION OF THE WORK
1660
DISTRIBUTE DIGITAL WORK THROUGH INFORMAL MEANS
1662
RELEGITIMIZATION SOFTWARE ATTACHES THE DOI TO THE WORK

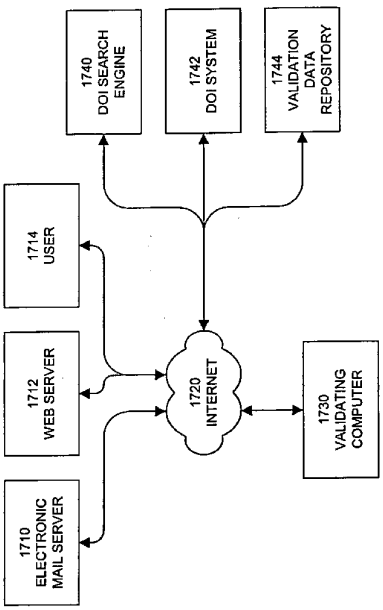

1740
DOI SEARCH
ENGINE
1742
DOI SYSTEM
1744
VALIDATION
DATA
REPOSITORY
1714
USER
1712
WEB SERVER
1720
INTERNET
1730
VALIDATING
COMPUTER
1710
ELECTRONIC
MAIL SERVER

Figure 17

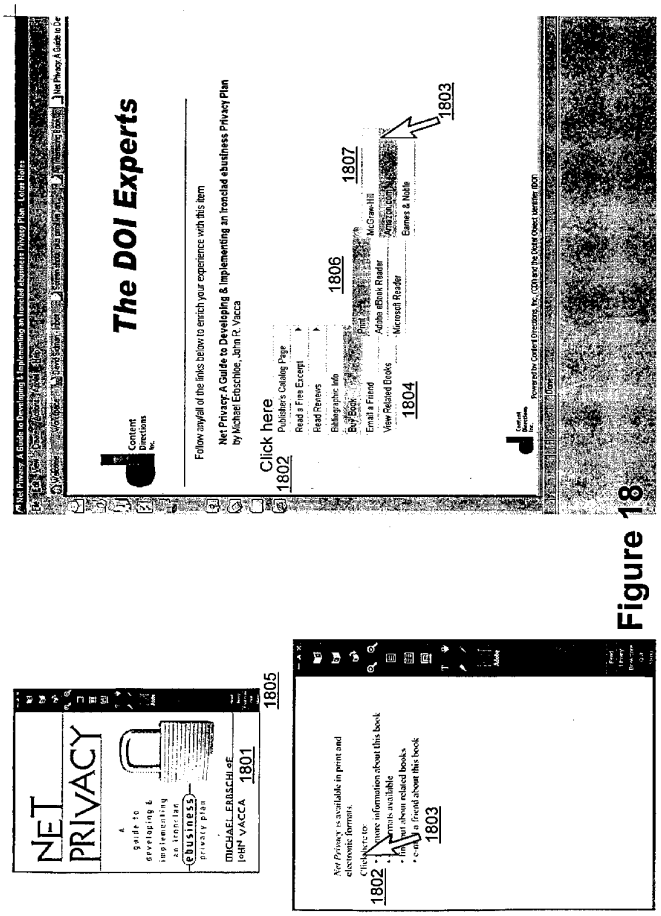

The DOI Experts
Follow any/all of the links below to enrich your experience with this item
Net Privacy: A Guide to Developing & Implementing an Ironclad eBusiness Privacy Plan
by Michael Erbschloe, John P. Vacca
Click here
1802
Publishers Catalog Page
Read a Free Excerpt
Read Reviews
Bibliographic Info
Email a Friend
View Related Books
1804
1806
1807
Adobe eBook Reader
Microsoft Reader
Barnes & Noble
1803
NET PRIVACY
A guide to developing & implementing an ironclad eBusiness privacy plan
MICHAEL ERBSCHLOE
JOHN P. VACCA
1801
1805
Net Privacy is available in print and electronic formats.
Click here to:
1802
Find more information about this book
Find out about related books
Email a friend about this book
1803

Figure 18

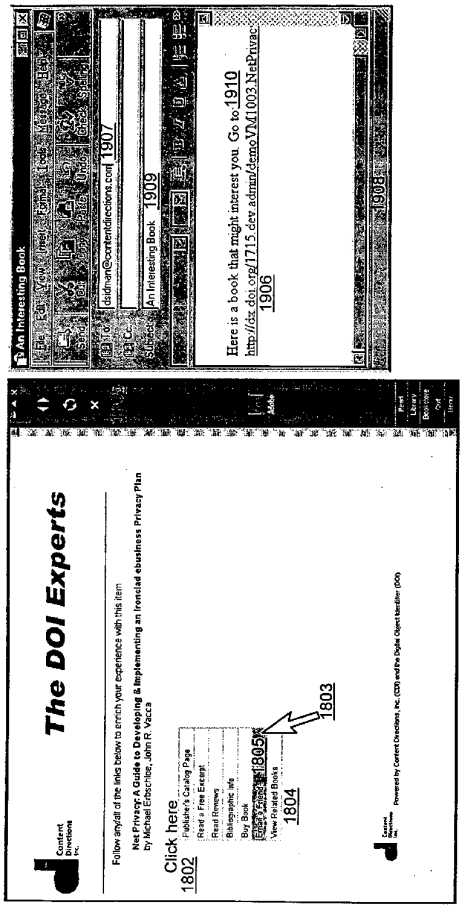

An Interesting Book
[doi:hom@contentdirections.com] 1907
An Interesting Book 1909
Here is a book that might interest you Go to 1910
http://dx.doi.org/1715.dev admin/demoVN41003.NetPrivac
1906
1908
The DOI Experts
Follow anyall of the links below to enrich your experience with this item
Net Privacy: A Guide to Developing & Implementing an Ironclad ebusiness Privacy Plan
by Michael Erbschloe, John R. Vacca
Click here
1802
Publisher's Catalog Page
Read a Free Excerpt
Read Reviews
Bibliographic Info
Buy Book
1805
View Related Books
1804
1803
Powered by Content Directions, Inc. (CDI) and the Digital Object Identifier (DOI)

Figure 19

【国際公開パンフレット（コレクトバージョン）】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 August 2002 (01.08.2002)

PCT

(10) International Publication Number
WO 02/060110 A3

(51) International Patent Classification⁷: G06F 13/00

(21) International Application Number: PCT/US02/02322

(22) International Filing Date: 25 January 2002 (25.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/264,333	25 January 2001 (25.01.2001)	US
60/267,875	8 February 2001 (08.02.2001)	US
60/267,899	9 February 2001 (09.02.2001)	US
60/268,766	14 February 2001 (14.02.2001)	US
60/270,473	21 February 2001 (21.02.2001)	US
60/276,459	16 March 2001 (16.03.2001)	US
60/279,792	29 March 2001 (29.03.2001)	US
60/303,768	10 July 2001 (10.07.2001)	US
60/328,275	9 October 2001 (09.10.2001)	US
60/328,274	9 October 2001 (09.10.2001)	US
60/328,270	9 October 2001 (09.10.2001)	US

(71) Applicant and
(72) Inventor: SIDMAN, David [US/US]; 558 9th Street, Brooklyn, NY 11215 (US).

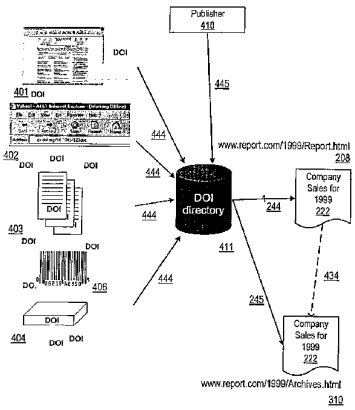
(74) Agent: HANCHUK, Walter, G.; Morgan & Finnegan, L.L.P., 345 Park Avenue, New York, NY 10154 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: APPARATUS, METHOD, AND SYSTEM FOR ACCESSING DIGITAL RIGHTS MANAGEMENT INFORMATION



(57) Abstract: Digital rights management (DRM) and content distribution systems need to reference unique works of authorship to facilitate distribution, access control, and usage tracking and reporting of the works. The apparatus, method, and system disclosed herein is a DRM and content distribution system that uses the digital object identifier (DOI) (401, 402, 403, 404) as a unique identifier for the works of authorship that are the subject of transactions within the system and that travel with the instantiations of the works of authorship. A method of accessing a digital work from a computer is disclosed. The method associates at least one usage right with the digital work to create a protected digital work. The usage rights include displaying the digital work, copying the digital work, fowarding the digital work to another computer, or printing the digital work. The method selects a unique identifier such as a DOI for the digital work and stores the protected digital work and the unique identifier in a directory (411) such as a library of digital works of autorship or a portion of a peer-to-peer network. The method issues a query from the computer to the directory to generate a result set that includes the unique identifier. The method uses the unique identifier to retrieve the protected digital work from the directory. Furthermore, a method is taught to employ multiple resolution capabilities for the super-distribution of DOI referenced content via E-mail and otherwise.

WO 02/060110 A3

WO 02/060110 A3

Published:
— *with international search report*

(88) Date of publication of the international search report:
30 January 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/02322

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 13/00
US CL : 713/153, 154, 200, 201
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/153, 154, 200, 201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WEST, INTERNET- search terms "Digital Object Identifiers" , "Digital Rights Management", "Handle System"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,135,646 A (KAHN et al) 24 October 2000 (24.10.2000) col. 2, line 17 to col. 5, line 22 and col. 5, line 61 to col. 28, line 28.	1-100
Y	KAHN, R., A Framework for Distributed Digital Object Services, Corporation for National Research Initiatives (CNRI), May 13, 1995.	1-100
Y	PASKIN, N, Digital Object Identifier: implementing a standard digital identifier as the key to effective digital rights management. International DOI Foundation, April 2000	1-100

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 24 August 2002 (24.08.2002)	Date of mailing of the international search report 17 SEP 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Matthew Smithers Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

フロントページの続き

(51)Int.Cl.[7]		FI			テーマコード（参考）
Ｈ０４Ｌ	9/32	Ｇ０６Ｆ	12/14	５３０Ａ	
Ｈ０４Ｎ	1/387	Ｇ０６Ｆ	12/00	５２０Ｅ	
		Ｇ０６Ｆ	12/00	５３７Ｈ	
		Ｇ０６Ｆ	15/00	３３０Ｅ	
		Ｇ０９Ｃ	1/00	６６０Ｄ	
		Ｇ０９Ｃ	5/00		
		Ｈ０４Ｎ	1/387		
		Ｈ０４Ｌ	9/00	６７３Ｃ	

(31)優先権主張番号 60/268,766
(32)優先日 平成13年2月14日(2001.2.14)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/270,473
(32)優先日 平成13年2月21日(2001.2.21)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/276,459
(32)優先日 平成13年3月16日(2001.3.16)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/279,792
(32)優先日 平成13年3月29日(2001.3.29)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/303,768
(32)優先日 平成13年7月10日(2001.7.10)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/328,275
(32)優先日 平成13年10月9日(2001.10.9)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/328,274
(32)優先日 平成13年10月9日(2001.10.9)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/328,270
(32)優先日 平成13年10月9日(2001.10.9)
(33)優先権主張国 米国(US)

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
イーサネット
フロッピー

【要約の続き】
ーを発行し、固有の識別子を含む結果を一セット生成する。当該方法は固有の識別子を用いて保護されたデジタル・ワークをディレクトリから入手する。更にまた、電子メール及びその他を介したＤＯＩで関連付けされたコンテンツ

の超流通のための多重解決能力を用いる方法を教示している。