

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号
特許第5095748号
(P5095748)

(45) 発行日 平成24年12月12日 (2012.12.12)

(24) 登録日 平成24年9月28日 (2012.9.28)

(51) Int. Cl.	F I
G O 6 K 19/06 (2006.01)	G O 6 K 19/00 E
H O 4 N 1/387 (2006.01)	H O 4 N 1/387
G O 6 T 1/00 (2006.01)	G O 6 T 1/00 5 O O B
G O 3 H 1/26 (2006.01)	G O 6 K 19/00 D
	G O 3 H 1/26

請求項の数 2 (全 12 頁)

(21) 出願番号 特願2009-537512 (P2009-537512)	(73) 特許権者 504142961
(86) (22) 出願日 平成19年11月13日 (2007.11.13)	バイエル・イノベーション・ゲゼルシャ
(65) 公表番号 特表2010-510596 (P2010-510596A)	フト・ミット・ベシュレンクテル・ハフツ
(43) 公表日 平成22年4月2日 (2010.4.2)	ング
(86) 国際出願番号 PCT/EP2007/009795	Bayer Innovation Gm
(87) 国際公開番号 W02008/061652	bH
(87) 国際公開日 平成20年5月29日 (2008.5.29)	ドイツ51373レーフェルクーゼン、カ
審査請求日 平成22年6月10日 (2010.6.10)	イザー・ヴィルヘルム・アレー20番
(31) 優先権主張番号 102006055480.9	(74) 代理人 100101454
(32) 優先日 平成18年11月24日 (2006.11.24)	弁理士 山田 卓二
(33) 優先権主張国 ドイツ (DE)	(74) 代理人 100081422
	弁理士 田中 光雄
	(74) 代理人 100125874
	弁理士 川端 純市

最終頁に続く

(54) 【発明の名称】 ホログラフィック記憶のための符号化方法、復号方法、コーデック及びデータ記憶媒体

(57) 【特許請求の範囲】

【請求項 1】

ホログラフィックデータ記憶媒体（4）上で保護する価値のある情報を暗号化するための符号化方法にしたがって暗号化された情報の項目を復号する復号方法において、

上記符号化方法は、
暗号化されるべき少なくとも1つの情報の項目（I；I₁，I₂）を提供するステップと、

上記情報を少なくとも2つのグラフィックデータイメージ（D₁，D₂）に変換するステップと、

上記グラフィックデータイメージ（D₁，D₂）を少なくとも2つのホログラム（H₁，H₂）に変換するステップと、

上記ホログラムを上記ホログラフィックデータ記憶媒体（4）に書き込むステップとを備え、

上記ホログラフィックデータ記憶媒体（4）に複数のホログラム（H'₁，H'₂）が書き込まれる前に、上記ホログラム（H₁，H₂）のグラフィックが上記ホログラム（H'₁，H'₂）に変更され、

上記復号方法は、
少なくとも1つのホログラム（H'₁，H'₂；H_{ges}）を有する上記ホログラフィックデータ記憶媒体（4）を提供するステップと、

レーザビームであるエネルギービームを上記ホログラフィックデータ記憶媒体（4）に

照射して、上記ホログラム ($H'_1, H'_2; H_{ges}$) を読み出すステップと、

上記ホログラフィックデータ記憶媒体 (4) で反射された上記エネルギービームを受信機 (5) で受信して、上記ホログラム ($H'_1, H'_2; H_{ges}$) をグラフィックデータイメージ (D_1, D_2) に変換するステップとを備え、

上記エネルギービームはフィルタ (2) に入射され、上記フィルタ (2) は、上記エネルギービームが 2 次元パターンで上記受信機 (5) に入射されるという方法で上記エネルギービームを部分的にのみ通過させ、上記 2 次元パターンは、イメージ鍵 (S_2) によって一意に定義されることを特徴とする復号方法。

【請求項 2】

ホログラフィック形式で存在する情報の項目を復号するコーデック回路において、

レーザビームであるエネルギービームを生成する放射源 (1) と、

上記エネルギービームをホログラフィックデータ記憶媒体 (4) に照射するレンズ (3) と、

上記ホログラフィックデータ記憶媒体 (4) を保持する保持デバイスと、

上記ホログラフィックデータ記憶媒体 (4) で反射された上記エネルギービームを検出する受信機 (5) とを備え、

上記保持デバイス及び上記レンズ (3) は、上記ホログラフィックデータ記憶媒体 (4) が複数の点で照射されうるような方法でお互いに相対的に移動されることが可能であり

、
上記エネルギービームのビーム経路上にフィルタ (2) は配置され、上記フィルタは、
上記エネルギービームを 2 次元パターンで上記受信機 (5) に照射するという方法で上記エネルギービームを変更し、上記 2 次元パターンは、イメージ鍵 (S_2) によって一意に定義されることを特徴とするコーデック回路。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、保護する価値のある情報を安全に記憶する方法に関し、その方法は、符号化方法及び復号方法を含む。さらに、本発明は、上記方法を実装する符号器 / 復号器 (“コーデック”)、及び上記符号化方法により生成された暗号化されたデータのホログラフィック記憶のためのデータ記憶媒体に関する。

【背景技術】

【0002】

情報を保護するために、一般に、情報はデジタルフォーマットに変換され、その後、実質的に利用された鍵の知識のみで復号できる暗号法の暗号化方法を用いて暗号化される。優れた暗号化の場合、暗号化された情報を復号するための鍵を計算機を用いて発見するための時間消費は非常に大きく、復号を実行する試みは権限のない人々にとって魅力がなくなる。なぜなら、さまざまな鍵を試すこと (“総当たり攻撃 (brute force attack)”)、例えば異なるパスワードが繰り返し試されることは、パスワードが多くの桁を有し対応して高いエントロピーを有している場合、非常に長時間継続するからである。しかしながら、この場合の不利な点は、デジタル形式で存在する暗号化された情報は何度も複製されうることであり、それにより、例えば、インターネットを経由して多くの異なる計算機に記憶され、可能な鍵の他の範囲がそれぞれの計算機で試されることが可能である (並列化された攻撃)。

【0003】

暗号化された情報の複製を防ぐために、コピー防止 (copy protection) を提供することが知られている。例えば、特許文献 1 は、暗号化された情報が記憶されている記憶媒体において、隠された特徴を提供することを開示しており、その特徴は、実際のデータが読み出される前に調査されるべきである。データ記憶媒体を複製する間、隠された特徴は、ファイルに属していないために見落とされ、その上、上記特徴は複製されず、その結果、複製は完全なものではない。しかしながら、このコピー防止は、複製プログラムが、デー

10

20

30

40

50

タとして識別される記憶媒体の領域だけでなく、使用されている領域と認識されるか使用されていない領域と認識されるかに関わらず記憶媒体のすべての領域を複製することによって回避されうる。したがって、コピー防止に関わらず、複数の異なる計算機で情報を復号するために、要望どおりの暗号化された情報の複製の数を準備することができる。

【 0 0 0 4 】

特許文献 2 は、ホログラムの生成の間、物体光（オブジェクトビーム）が、物体光（オブジェクトビーム）の上に重畳されたランダムに変調された参照光（リファレンスビーム）を有するホログラフィックデータ記憶を提供することを開示する。これは、記憶されるべき情報の光暗号化をもたらす。同一の変調が読み出すときに使用されなければならない。この符号化方法の不利な点は、変調された参照光（リファレンスビーム）を提供するために、特に摩耗現象、及びとりわけ正確な制御された位置に対する必要条件によって相応に障害の影響を受けやすい可動部品を有する機構が要求されることである。例えば、使用している装置に対する非常に小さいノックの結果発生しうるような、ホログラムの生成の間の単一の非常に小さいエラーでさえ、損傷した情報をもたらし、その情報は権限のあるユーザによってさえ、もはや再構成することができない。

10

【先行技術文献】

【特許文献】

【 0 0 0 5 】

【特許文献 1】欧州特許出願公開第 1 3 5 5 2 1 7 号公報。

【特許文献 2】米国特許第 3 8 9 4 7 5 6 号明細書。

20

【発明の概要】

【発明が解決しようとする課題】

【 0 0 0 6 】

本発明の目的は、並列化された総当たり攻撃に対するより高い耐性を示し、障害に対する感受性の減少によって扱いやすいホログラフィック記憶に対する符号化方法、復号方法、コーデック及びデータ記憶媒体を提供することである。

【課題を解決するための手段】

【 0 0 0 7 】

本発明によれば、上記目的は請求項 1 記載の特徴を有する符号化方法、請求項 8 記載の特徴を有する復号方法、請求項 1 3 記載の特徴を有するコーデック、及び請求項 1 7 記載の特徴を有するデータ記憶媒体によって達成される。本発明のさらなる改良は、下位クレームに明記されている。

30

【 0 0 0 8 】

ホログラフィックデータ記憶媒体上で保護する価値のある情報を暗号化する本発明に係る符号化方法では、まず第 1 に、暗号化された情報の項目が提供され、上記情報は、特にデジタルフォーマットで存在している。暗号化されるべき情報の項目はまた、より大きい全体の情報の項目の相対的に小さい部分でもよい。その後、情報は、少なくとも 1 つのグラフィックデータイメージに変換され、それにより上記情報は、グラフィックフォーマットで存在している。例えば、データイメージは、白及び黒の矩形の列で構成され、それぞれの矩形は、デジタル形式で存在する情報の 1 ビットに対応する。データ密度を増加させるために、複数の異なる色、又はグレーステップ（gray steps）が使用されることも可能である。その後、グラフィックデータイメージは、ホログラムでホログラフィックデータ記憶媒体を書き込むために、少なくとも 1 つのホログラムに変換される。ホログラムは、特に、例えば反復フーリエ変換アルゴリズム（IFTA：Iterative Fourier Transformation Algorithm）を用いて計算機で生成されることによって得られる。

40

【 0 0 0 9 】

本発明によれば、ホログラフィックデータ記憶媒体がホログラムで書き込まれる前に、ホログラムはグラフィックで変更される。ホログラムにおけるグラフィック変更は、別の暗号化レベルを表し、その暗号化はデジタル暗号化から独立している。事前に実行された

50

デジタル暗号化方法を復号するパスワードの知識を有していても、まだ実用的な情報は、ホログラフィックデータ記憶媒体から集められることができない。その結果、特にある計算機から別の計算機への暗号化された情報の伝送は、より良く保護され、それにより、ホログラフィックデータ記憶媒体が権限のない者へ渡っても、暗号化された情報はまだ失われない。ホログラムにおけるグラフィック変更は、例えば特に自己消去 (self-deleting) プログラムを用いて、可逆にすることができ、本プログラムが異なるルートにより送信先の計算機へ到達することが可能である。例えば、ホログラムは、郵便で発送されたホログラフィックデータ記憶媒体上に記憶されることができ、一方、グラフィック変更を可逆にする復号プログラムは、個別に配分されることが可能な登録番号の入力に続いて、インターネットを経由してダウンロードされることができる。ホログラムにおけるグラフィック変更は、特に計算機で生成されたホログラムの場合、特に簡単に実行されることから、保護する価値のある情報の復号に対する改善された保護は、障害の影響をほとんど受けない単純な方法を用いて達成される。ホログラムにおけるグラフィック変更は、情報を解体し再配置することから、元の情報に対してシーケンシャルに順序付けされていない暗号化が達成され、これにより、並列化された総当たり攻撃を用いた復号は、少なくとも相当により難しくなる。ホログラムは、ホログラフィックデータ記憶媒体が書き込まれる前に、グラフィックで変更されることから、複雑で障害の影響を受けやすい使用されるべきデータの機構は、書き込み操作に対して避けられる。

【 0 0 1 0 】

本発明に係る符号化方法の好ましい実施形態において、グラフィックデータイメージは、グラフィックデータイメージを変換する間に、少なくとも2つの部分領域へ分割される。その後、部分領域は、好ましく定義された順序で2次元パターンの形式のホログラムに変換され、上記2次元パターンは、イメージ鍵を用いて一意に定義される。その後、ホログラフィックデータ記憶媒体は、上記ホログラムで書き込まれる。イメージ鍵において、個別の部分領域が処理される順序を定義することができる。例えば、複数の矩形の部分領域で構成される長方形のデータイメージは、行ごとに、列ごとに、又は部分領域の任意の所望の順序で処理されることができる。さらに、イメージ鍵において、それぞれの部分領域は、その初期位置に関して、移動及び/又は回転を割り当てられることができる。例えば、長方形のデータイメージは、複数の等しいサイズの矩形の部分領域に分割され、特定の部分領域が、定義された数の部分領域によって水平方向及び/又は垂直方向へ移動されること、及び/又は特に90°の倍数で回転されることが可能である。グラフィックデータイメージを変換する間、部分領域が変換されたデータイメージにおいて重複するのであれば、データ密度が、例えば、解像度がそれらの領域において適切に増加させられること、あるいはより多くのグレーステップ (gray steps) が許可されることによって、必要ならばそれらの領域において増加させられることが可能である。

【 0 0 1 1 】

追加又は代替として、グラフィックデータイメージは、中間ステップにおいて中間ホログラムに変換されることができ、この中間ホログラムは少なくとも2つの部分領域に分割され、その後、それら部分領域は、一意に2次元パターンを定義するイメージ鍵を用いて、特に定義された順序で2次元パターンの形式のホログラムに変換される。上記変換は、特に、データイメージの変換を用いることによって、上述したように実行されることができる。その後、この方法で生成されたホログラムは、ホログラフィックデータ記憶媒体へ書き込まれる。イメージ鍵は、例えば、グラフィックデータイメージ、及び/又は中間ホログラムが分割される部分領域の数、2次元パターンがどのような形及び配置を有しているのか、さらにどの部分領域がパターンのどのポイントで配置されるのかに関する情報を含む。部分領域の数は、異なって配置された2次元パターンがいくつ可能かということに影響し、その方法で、部分領域が2次元パターンへ整列される。部分領域の数、及び/又はパターンの数は、特に、エントロピー、つまり暗号化の複雑度が最大となるような方法で選択される。

【 0 0 1 2 】

グラフィックで変更されたホログラム、つまり２次元パターンは、特に、グラフィック変更なしでグラフィックデータイメージが変換された中間ホログラム、又はホログラムと同一の外部の輪郭を有しない。グラフィックデータイメージは、通常、できるだけ密度が高く密集して構成されるため、この方法によりグラフィックで変更されたホログラムは、未使用の空間を有する２次元パターンとなる。これら未使用の空間は、好ましくは、例えば関連のない干渉情報であるホログラフィックデータで充填される。空間が充填されるという事実は、暗号化された情報を有するホログラムの２次元パターンが、ホログラフィックデータ記憶媒体のどのような試験によっても決定できないことを意味する。特に好ましくは、未使用の空間は、別の暗号化された情報の項目から生成された別のホログラムで少なくとも部分的に充填される。この場合、この別のホログラムのグラフィック変更は、特にグラフィックで変更されたホログラムの生成の間に使用された事前に使用されたイメージ鍵を考慮しながら実行される。このことは、ホログラムが重複しないこと、及び情報が不注意に破壊されないことを保障する。正確に２つのグラフィックで変更されたホログラムが、お互いに入れ子にされることがあれば、第２のホログラムを暗号化するイメージ鍵は、第１のホログラムを暗号化するイメージ鍵の逆バージョンにある。特に好ましくは、複数のホログラムが、例えば標準化されたサイズのホログラムブロックを作り出すために、お互いに入れ子にされる。多数のホログラムがお互いに入れ子にされた結果、複数のイメージ鍵が必要とされ、それにより暗号化の複雑度が、特に単純な方法で増加する。

【００１３】

ホログラフィックデータ記憶媒体に記憶されたホログラムは、例えば振幅ホログラム、又は偏光ホログラムとして記憶されてもよい。振幅ホログラムは、“密着焼付け（contact printing）”方法により複製できることから、偏光ホログラムが好まれる。偏光ホログラムが、ホログラムでホログラフィックデータ記憶媒体を書き込むことによって生成されると、ホログラフィックデータ記憶媒体を複製することは、より困難になる。特に、ホログラフィックデータ記憶媒体を複製するためには、光学的に偏光ホログラムを読み出すためにまず設置され調整されなければならない光学システムが必要とされる。これは、デジタル形式で存在するデータと比較して、相当により時間がかかるため、ホログラフィックデータ記憶媒体の大量複製は、相当に増加した時間消費のために、より困難になる。フォトアドレス割当可能なポリマーは偏光ホログラムの記憶を可能にすることから、特に好ましくはこれらがホログラフィックデータ記憶媒体に利用される。

【００１４】

暗号化の複雑度をさらに増加させるために、好ましくは暗号化されるべき情報を少なくとも２つの情報の部分項目へ分割することが行われ、イメージ鍵あるいは異なるイメージ鍵を用いてそれぞれのケースにおいて、本方法の別のコースにおいて個別に、それぞれの情報の部分項目を暗号化する。特に好ましくは、暗号化されるべき情報は、少なくとも２つの部分ブロックに事前に分割され、それらブロックは、情報鍵を用いて情報の部分項目に分割される。例えば、暗号化されるべき情報は、等しい又は異なる長さの複数の部分ブロックに分割され、部分ブロックは、特定の順序で交互に又は異なる方法にしたがって、少なくとも２つの情報の部分項目に分割される。その結果、情報は複数の部分に解体され、生成された情報の部分項目内に再配置されることから、保護する価値のある情報に対する追加の暗号化が達成される。

【００１５】

好ましくは、情報あるいは情報の部分項目を少なくとも１つのグラフィックデータイメージに変換する間、グラフィックデータイメージの数、サイズ、ラスタリングを定義する変換鍵が使用される。情報もまた、１つ以上のグラフィックデータイメージに変換されるという事実は、暗号化の複雑度が増加しうることを意味する。さらに、選択されたグラフィックデータイメージのラスタリング、つまりデジタル形式で存在する情報の項目の１ビットに対応する２次元領域がどれほど小さいか又は大きいかは、対応して物理的に実行されなければならない読み取り機の設定を必要にする。さまざまな設定を試みるために必要とされる時間消費は、記憶されたホログラムの復号を魅力がないものにする。特に、干渉

情報がデータイメージ中に提供されており、データイメージのラスタリングが暗号化された情報の区切りの2倍細かいものであれば、権限のないユーザは細かすぎるラスタと仮定したくなり、それによりホログラムは、対応するデジタル形式へ復号されることができない。

【0016】

本発明は、さらに、上述した符号化方法で暗号化された情報を復号することができる復号方法に関する。本発明に係る復号方法では、まず、少なくとも1つのホログラムを有するホログラフィックデータ記憶媒体が提供される。その後、ホログラフィックデータ記憶媒体は、ホログラムを読み出すために、特にレーザビームであるエネルギービームを用いて照射される。ホログラフィックデータ記憶媒体で反射されたエネルギービームは、ホログラムをグラフィックデータイメージに変換するために、受信機を用いて受信される。本発明によれば、エネルギービームはフィルタに入射され、そのフィルタはエネルギービームを部分的にのみ通過させる。エネルギービームは2次元パターンで受信機に入射されるという方法でフィルタを通過し、その2次元パターンはイメージ鍵によって一意に定義される。

10

【0017】

フィルタによって反射、及び/又は吸収されるエネルギービームの部分は、復号されるべき情報の項目の再構成に関係しないホログラフィックデータ記憶媒体に記憶されたホログラムの部分に対応する。エネルギービームに対するステンシルのようなフィルタリングを用いることで、復号されるべき情報に対応するホログラムの部分のみが受信機によって受信される。ホログラムにおけるグラフィック変更のために利用されたイメージ鍵は、イメージ鍵で定義される2次元パターンに関するフィルタで明示される。フィルタは、ホログラムを復号する間に適切な装置へ単純に挿入されることができる構成部品となることができる。限定された数のフィルタのみしかない場合、暗号化された情報を保護することをフィルタの監視によって、一般に、使用されたホログラフィックデータ記憶媒体の単なる不完全な監視がセキュリティに関してほとんどなくなるように、確立することができる。

20

【0018】

好ましくは、エネルギービームは、すでに2次元パターンで、ホログラフィックデータ記憶媒体に入射される。したがって、好ましくは、フィルタは入力されるエネルギービームのビーム経路に配置され、反射されたエネルギービームのビーム経路には配置されない。おそらく、不利な散乱効果はそれによって避けられる。さらに、ホログラフィックデータ記憶媒体の部分照射は、より簡単に調査されることができる。

30

【0019】

好ましい実施形態において、使用されたフィルタは液晶ディスプレイであり、又は液晶ディスプレイを有するフィルタが使用される。液晶ディスプレイを用いることで、特に物理的にエネルギービームの振幅を変化させるフィルタは、特に単純に異なる2次元パターンを設定することができる。したがって、同一のフィルタは、さまざまなイメージ鍵の2次元パターンをエネルギービームへ印加することができる。特に好ましくは、液晶ディスプレイは、少なくとも1つのイメージ鍵が記憶された計算機ユニットへ接続される。その結果、液晶ディスプレイによって印加されるパターンは、計算機ユニットに記憶されたイメージ鍵に応じて生成されることができる。これは、特に、柔軟に利用できる技術に興味を持つユーザに対して、本発明に係る復号方法の商用アプリケーションを可能にする。

40

【0020】

本発明は、さらに、符号器/復号器(“コーデック”)、つまりホログラフィック形式で存在する情報の項目を符号化する、及び/又は復号するデバイスに関する。コーデックは、エネルギービーム、特にレーザビームを生成する放射源を有する。レンズ配置を用いて、ホログラフィックデータ記憶媒体は、エネルギービームを用いて照射されることができる。さらに、コーデックは、ホログラフィックデータ記憶媒体を保持する保持デバイスを有する。保持デバイス、及びレンズ配置は、ホログラフィックデータ記憶媒体が、複数の点で、特に一面のすべての点で照射されうるような方法で、お互いに相対的に移動され

50

ることができる。さらに、受信機は、ホログラフィックデータ記憶媒体から反射されたエネルギービームを検出するために提供される。本発明によれば、フィルタは、エネルギービームのビーム経路に配置され、エネルギービームが２次元パターンで受信機を照射するようにエネルギービームを変更し、その２次元パターンは、イメージ鍵によって一意に定義される。本発明に係るコーデックは、特に、符号化方法、及び／又は復号方法を用いて上述したように設計され開発される。

【００２１】

本発明は、さらに、暗号化されたデータのホログラフィック記憶のためのデータ記憶媒体に関し、データ記憶媒体はホログラムを記憶するデータ記憶素子を有する。本発明によれば、データ記憶素子は２次元パターンの形式を有する複数のホログラムを有する。２次元パターンはイメージ鍵によって一意に定義される。したがって、ホログラムは、データ記憶素子の中で、順序付けられて連続して配置されていないことから、記憶されたデータの暗号化は、単純な方法によって達成される。イメージ鍵の知識によってのみ、情報が記憶されたデータ記憶素子の関係ある領域が決定されることができる。

【００２２】

好ましくは、データ記憶素子は、複数の標準化されたサイズのホログラムブロックを有し、ホログラムブロックは、情報の項目に関する少なくとも２つのホログラムを有する。ホログラムは、特に、未使用の中間領域が避けられるような方法で、お互いに入れ子にされる。このようにして、２次元パターンの形式は、覆い隠される。

【００２３】

特に好ましくは、データ記憶素子は、フォトアドレス割当可能なポリマーを持つフィルムを有する。特に、フォトアドレス割当可能なポリマーを用いて、好ましくは偏光ホログラムとしてデータ記憶素子にホログラムを記憶することができる。その結果、データ記憶媒体の複製が回避される。

【００２４】

以下、本発明は、添付の図を参照してより詳細に説明される。

【図面の簡単な説明】

【００２５】

【図１】本発明に係る符号化方法の第１のステップを示す。

【図２】本発明に係る符号化方法の第２のステップを示す。

【図３】本発明に係る符号化方法の第３のステップを示す。

【図４】本発明に係る符号化方法の第４のステップを示す。

【図５】本発明に係る復号方法の第１及び第２のステップを示す。

【図６】本発明に係る復号方法の第３のステップを示す。

【図７】本発明に係るコーデックの概略図を示す。

【発明を実施するための形態】

【００２６】

本発明に係る符号化方法の第１のステップ（図１）において、情報の項目 I は、２つの情報の部分項目 I_1 , I_2 に分割される。情報の項目 I を２つの情報の部分項目 I_1 , I_2 へ分割する間に第１の暗号化をすでに達成するために、情報の項目 I は、複数の部分ブロックへ分割され、図１の部分ブロックは、下線が引かれた数字、及び下線が引かれていない数字を用いて次々に示される。情報の項目 I を２つの情報の部分項目 I_1 , I_2 へ分割する間に、下線が引かれた数字で示される部分ブロックは、情報の部分項目 I_2 へ割り当てられ、下線が引かれていない数字で示される部分ブロックは、情報の部分項目 I_1 へ割り当てられる。情報の項目 I を少なくとも２つの情報の部分項目 I_1 , I_2 へ後に配分するために情報の項目 I が部分ブロックへ分割される方法は、情報鍵 S_1 によって定義される。

【００２７】

符号化方法の第２のステップ（図２）において、情報の部分項目 I_1 , I_2 は、グラフィックデータイメージ D_1 , D_2 にそれぞれ変換される。グラフィックデータイメージ D

10

20

30

40

50

D_1 , D_2 はバーコードであってもよい。好ましくは、グラフィックデータイメージ D_1 , D_2 はマトリックスコードである。なぜなら、マトリックスコードはバーコードよりも同一の面に対する必要条件で、より多くの情報を符号化できるからである。説明される例示的な実施形態において、グラフィックデータイメージ D_1 , D_2 は、白及び黒の矩形の列から組み立てられ、それぞれの矩形は、デジタル形式で存在する情報の項目 I_1 , I_2 の 1 ビットに対応する。使用されるグラフィックデータイメージ D_1 , D_2 のサイズ、及び白ならびに黒の矩形のサイズ（ラスティング（rastering））は、変換鍵 S_3 によって定義される。さらに、情報の部分項目 I_1 , I_2 を変換する間に、個別の部分ブロックへの分割は、情報鍵 S_1 を用いて上述したように、即座に実行される（図 1）。

【 0 0 2 8 】

10

符号化方法の第 3 のステップ（図 3）において、グラフィックデータイメージ D_1 , D_2 は、計算機で生成された中間ホログラム H_1 , H_2 に変換される。この変換は、特に、反復フーリエ変換アルゴリズム（IFTA）などの計算機で生成されたホログラムの生成に対する標準化された方法によって実行される。しかしながら、例えばさらなる暗号化を達成するために IFTA から変更された、具体的に構成されたアルゴリズムを使用することも可能である。

【 0 0 2 9 】

符号化方法の第 4 のステップ（図 4）において、中間ホログラム H_1 , H_2 は、イメージ鍵 S_2 を用いて、ホログラム H'_1 , H'_2 に変換される。この変換のために、第 1 の中間ホログラム H_1 は、複数の部分領域 $h_{1,1}, h_{1,2}, \dots, h_{1,n}$ へ分割される。これらの部分領域 $h_{1,1}, h_{1,2}, \dots, h_{1,n}$ は、定義された順序で 2 次元パターンの形式へ配置され、第 1 のホログラム H'_1 となる。第 2 の中間ホログラム H_2 は、対応した方法で処理され、部分領域 $h_{2,1}, h_{2,2}, \dots, h_{2,n}$ は、定義された順序で 2 次元パターンの形式へ配置され、この順序は、第 1 のホログラム H'_1 の 2 次元パターンに関して反転されている。したがって、第 1 のホログラム H'_1 の 2 次元パターン、及び第 2 のホログラム H'_2 の 2 次元パターンは、未使用の空間が避けられるような方法で、お互いに入れ子にされることができ、ホログラムブロック H_{ges} となり、ホログラムブロック H_{ges} では、ホログラム H'_1 , H'_2 の 2 次元パターンは見られない。イメージ鍵 S_2 によって一意に定義されるホログラム H'_1 , H'_2 の 2 次元パターンは、ホログラムブロック H_{ges} において完全に隠蔽されている。

20

30

【 0 0 3 0 】

ホログラムブロック H_{ges} に記憶された情報を復号するために（図 5）、ホログラム H'_1 , H'_2 の 2 次元パターンの知識が所与とすると、まず、例えばフィルタを用いて、2 次元パターンのうちの 1 つが覆われることができ、イメージ鍵 S_2 を用いることによってのみ第 1 のホログラム H'_1 が第 1 のデータイメージ D_1 へ変形し戻されることができる。その後、第 1 のグラフィックデータイメージ D_1 は、変換鍵 S_3 を用いて、第 1 の情報の部分項目 I_1 に変換し戻されることができる。第 2 のホログラム H'_2 は、対応する方法で処理され、この場合、ホログラム H'_1 の 2 次元パターンは覆われ、第 2 のホログラム H'_2 のみが見える。

【 0 0 3 1 】

40

復号方法の最後のステップ（図 6）において、情報の部分項目 I_1 , I_2 は、情報鍵 S_1 を用いて、所望の暗号化されていない情報の項目 I へ変更される。

【 0 0 3 2 】

符号化方法、及び復号方法を実行するために、コーデック（図 7）は、例えばレーザー光線を生成する放射源 1 を有する。このエネルギービームは、レンズ配置 3 を経由して、ホログラフィックデータ記憶媒体 4 上へ偏向される。ホログラフィックデータ記憶媒体 4 は、實際上ホログラフィックデータ記憶媒体 4 のすべての領域が照射されるように、保持デバイスの中に配置される。ホログラフィックデータ記憶媒体 4 から反射された光は、グラフィックデータイメージ D_1 , D_2 へ読み込まれているホログラム H'_1 , H'_2 を変換するために、受信機 5 によって検出される。フィルタ 2 は、エネルギービームのビーム経

50

路、特にエネルギービームがホログラフィックデータ記憶媒体 4 へ入射される前に配置される。説明される例示的な実施形態において、フィルタ 2 は、第 2 のホログラム H'_2 の 2 次元パターン（上）、又は第 1 のホログラム H'_1 の 2 次元パターン（下）のどちらかを除去する。この 2 次元パターンは、イメージ鍵 S_2 によって一意に定義される。異なる 2 次元パターンの間で特に単純に変更ができるように、フィルタ 2 は、液晶ディスプレイを有することができ、その液晶ディスプレイは、要求に応じて適切な 2 次元パターンを設定する。この目的を達成するために、液晶ディスプレイは、計算機ユニットに接続されることができ、その計算機ユニットにイメージ鍵 S_2 が記憶されている。

【図 1】

BIG 06 | 011-Foreign Countries

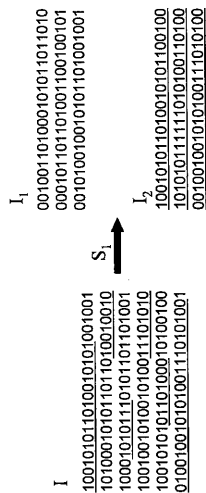


Fig. 1

【図 2】

BIG 06 | 011-Foreign Countries

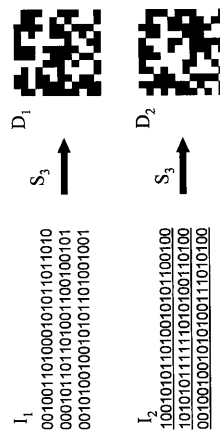


Fig. 2

【 図 3 】

BIG 06.1.011-Foreign Countries

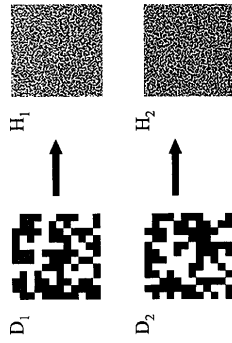


Fig. 3

【 図 4 】

BIG 06.1.011-Foreign Countries

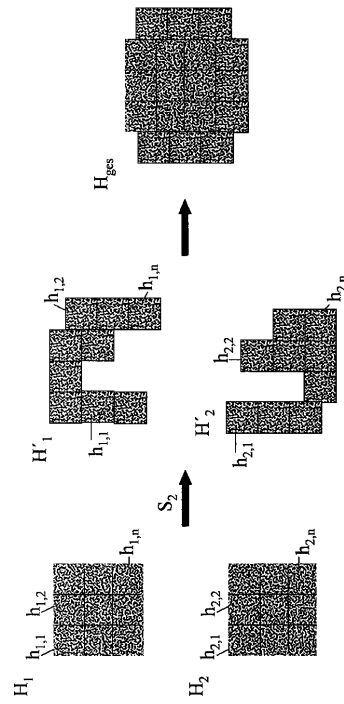


Fig. 4

【 図 5 】

BIG 06.1.011-Foreign Countries

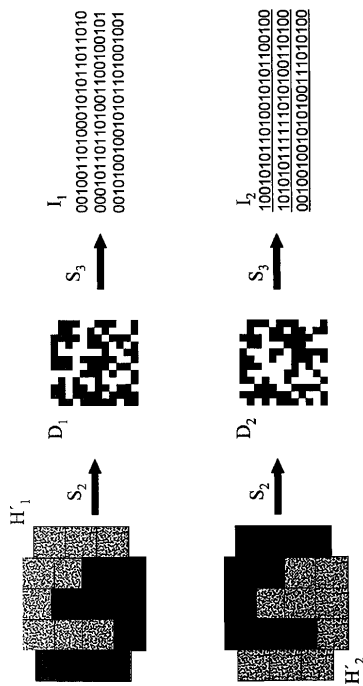


Fig. 5

【 図 6 】

BIG 06.1.011-Foreign Countries

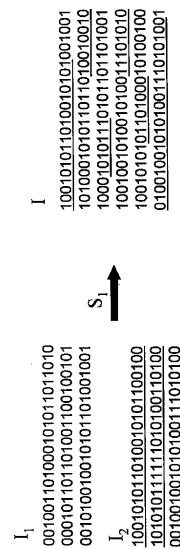


Fig. 6

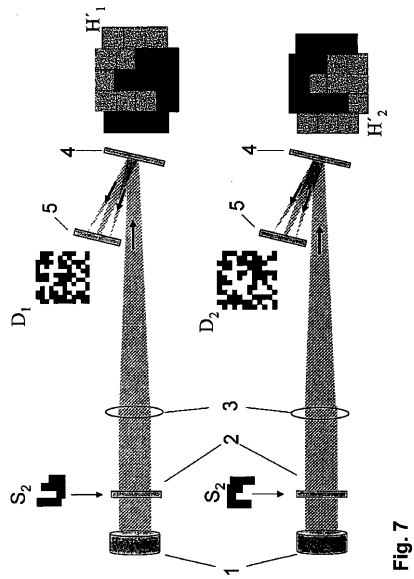


Fig. 7

フロントページの続き

(72)発明者 ジャン - ミシェル・アスフル

ドイツ連邦共和国デー - 6 9 4 6 9 ヴァインハイム、クリームヒルトシュトラッセ 1 1 番

審査官 和田 財太

(56)参考文献 特開 2 0 0 0 - 1 2 3 1 3 3 (J P , A)

特開 2 0 0 2 - 0 3 6 7 6 3 (J P , A)

特開 2 0 0 0 - 1 8 2 2 3 8 (J P , A)

特開平 0 7 - 0 6 5 1 3 8 (J P , A)

特開平 1 0 - 1 9 0 4 7 3 (J P , A)

(58)調査した分野(Int.Cl. , D B 名)

G06K 19/06

G03H 1/26

G06T 1/00

H04N 1/387