(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4832692号
(P4832692)

(45)発行日　平成23年12月7日(2011.12.7)　(24)登録日　平成23年9月30日(2011.9.30)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	560C
H04N 5/91	(2006.01)	H04N	5/91	P
H04N 1/387	(2006.01)	H04N	1/387	
G09C 5/00	(2006.01)	G09C	5/00	

請求項の数 44　(全 30 頁)

(21)出願番号	特願2001-533740 (P2001-533740)
(86)(22)出願日	平成12年10月27日 (2000.10.27)
(65)公表番号	特表2003-513364 (P2003-513364A)
(43)公表日	平成15年4月8日 (2003.4.8)
(86)国際出願番号	PCT/US2000/029843
(87)国際公開番号	WO2001/031910
(87)国際公開日	平成13年5月3日 (2001.5.3)
審査請求日	平成19年10月29日 (2007.10.29)
(31)優先権主張番号	09/437,713
(32)優先日	平成11年10月28日 (1999.10.28)
(33)優先権主張国	米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100089705
弁理士　社本　一夫
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100080137
弁理士　千葉　昭男
(74)代理人　100096013
弁理士　富田　博行

最終頁に続く

(54)【発明の名称】デジタルデータのフィンガープリンティングのための方法およびシステム

(57)【特許請求の範囲】

【請求項１】

Γコードを形成するためにコンピュータによって実施される方法であって、

各々が一意でありかつ少なくとも1つの拡散シーケンスを含む複数のフィンガープリンティングワードを構築して、関連するフィンガープリンティングワードを変更する潜在的な共謀者の身元を確認する共謀者の解析を可能にするステップであって、各フィンガープリンティングワードは複数のΓシンボルを含み、各Γシンボルは２ｃ－１個（ここで、ｃは防御したい共謀者の人数である）の拡散シーケンスを含むステップと、

個々のフィンガープリンティングワードを、潜在的な共謀者を構成する個々のそれぞれのユーザに割り当てて、前記フィンガープリンティングワードを、それを割り当てられたユーザを識別するのに用いるステップと

を備えることを特徴とする方法。

【請求項２】

フィンガープリンティングワードを検出するためにコンピュータによって実施される方法であって、

個々の拡散シーケンスを定義する個々のブロックに配列された複数のスペクトル拡散チップを含むフィンガープリンティングワードをその中に埋め込んだ被保護オブジェクトを受信するステップと、

前記フィンガープリンティングワードに関連付けられる、潜在的な共謀者を含むユーザを識別するのに充分に前記被保護オブジェクトを処理するステップと

を備え、
前記処理するステップは、
元の拡散シーケンスブロック値の１の補数に対する各ブロックの重みを計算して、各ブロックが可視である可能性が高いか、不可視である可能性が高いかを決定するステップと、
特定の前記ブロックが不可視である可能性が高いと決定されたならば、前記特定のブロックの前記重みを予め定められた値に制限するステップと
を備えることを特徴とする方法。
【請求項３】
前記制限するステップは、ブロックが不可視である可能性が高い場合にそうすることを備えることを特徴とする、請求項２に記載の方法。
【請求項４】
前記予め定められた値は（１－δ）μに等しく、ここで、Ｎ人のユーザの場合、誤り発生確率εでサイズｃの共謀を防御するために、
フィンガープリンティングワード当たりのΓシンボルの数＝Ｌ＝２ｃｌｎ（２Ｎ／ε）
ブロックサイズ(チップで測定)＝ｄ＝８ｃ^{2}ｌｎ（８ｃＬ／ε）
ｆ＝２ｌｎ（４ｃ^{2}ｌｎ（２Ｎ／ε）／ε）
δ＝ｆ／√（ｄ／２）
μ＝ｄ／２
を選択することを特徴とする、請求項２に記載の方法。
【請求項５】
前記埋め込まれたフィンガープリンティングワードは、各々複数のブロックを含む複数のΓシンボルを有し、複数のユーザの各々は複数のΓシンボルを有する一意のフィンガープリンティングワードを割り当てられ、
前記処理するステップは、
前記埋め込まれたフィンガープリンティングワードの各Γシンボルについて、共謀の対象である可能性のある1つまたは複数の色のセットを決定するステップと、
前記ユーザのフィンガープリンティングワードの各々について、各Γシンボルを評価して、それが、前記埋め込まれたフィンガープリンティングワードの対応するΓシンボルのセット内の色と一致するか否かを確認するステップと、
最大数の色を有するユーザを選択するステップと
を備えることを特徴とする、請求項２に記載の方法。
【請求項６】
前記決定するステップは、
各ブロックの重みを評価するステップと、
前記ブロックの重みが予め定められた関係を満たす場合、Γシンボルを選択するステップと
を備えることを特徴とする、請求項５に記載の方法。
【請求項７】
コンピュータによって実行されたときに請求項６に記載の方法を実行するコンピュータ実行可能命令をその中に有することを特徴とするコンピュータ可読媒体。
【請求項８】
オブジェクトを保護するためにコンピュータによって実施される方法であって、
各々が一意でありかつ少なくとも1つの拡散シーケンスを含む複数のフィンガープリンティングワードを構築して、関連するフィンガープリンティングワードを変更する潜在的な共謀者を含むユーザの身元を確認する共謀者の解析を可能にするステップであって、前記フィンガープリンティングワードは各々複数の拡散シーケンスを含み、各フィンガープリンティングワードの拡散シーケンスは個々のブロックに配列されるステップと、
個々のフィンガープリンティングワードを個々の前記ユーザに割り当てて、前記フィンガープリンティングワードを、それを割り当てられたユーザを識別するのに用いるステッ

プと、
複数のオブジェクトにそれぞれの個々のフィンガープリンティングワードを埋め込んで個々の被保護オブジェクトを提供するステップと、
前記被保護オブジェクトを前記個々のユーザに配布するステップと、
被保護オブジェクトを受信するステップと、
前記被保護オブジェクトを充分に処理して、前記受信した被保護オブジェクトに含まれるフィンガープリンティングワードに関連付けられるユーザを識別するステップと
を備え、
前記処理するステップは、
元の拡散シーケンスブロック値の１の補数に対する各ブロックの重みを計算して、各ブロックが可視である可能性が高いか、不可視である可能性が高いかを決定するステップと、
特定の前記ブロックが不可視である可能性が高いと決定されたならば、前記特定のブロックの前記重みを予め定められた値に制限するステップと
を備えることを特徴とする方法。
【請求項９】
前記制限するステップは、ブロックが不可視である可能性が高い場合にそうすることを備えることを特徴とする請求項８に記載の方法。
【請求項１０】
前記予め定められた値は（１－δ）μに等しく、ここで、Ｎ人のユーザの場合、誤り発生確率εでサイズｃの共謀を防御するために、
フィンガープリンティングワード当たりのΓシンボルの数＝Ｌ＝２ｃｌｎ（２Ｎ／ε）
ブロックサイズ(チップで測定)＝ｄ＝８ｃ^{2}ｌｎ（８ｃＬ／ε）
ｆ＝２ｌｎ（４ｃ^{2}ｌｎ（２Ｎ／ε）／ε）
δ＝ｆ／√（ｄ／２）
μ＝ｄ／２
を選択することを特徴とする、請求項８に記載の方法。
【請求項１１】
前記埋め込まれたフィンガープリンティングワードは、各々複数のブロック含む複数のΓシンボルを有し、複数のユーザの各々が複数のΓシンボルを有する一意のフィンガープリンティングワードを割り当てられ、
前記処理するステップは、
前記埋め込まれたフィンガープリンティングワードの各Γシンボルについて、共謀の対象である可能性のある1つまたは複数の色のセットを決定するステップと、
前記ユーザのフィンガープリンティングワードの各々について、各Γシンボルを評価して、それが、前記埋め込まれたフィンガープリンティングワードの対応するΓシンボルのセット内の色と一致するか否かを確認するステップと、
最大数の色を有するユーザを選択するステップと
を備えることを特徴とする、請求項８に記載の方法。
【請求項１２】
コンピュータに、
各々が一意でありかつ少なくとも1つの拡散シーケンスを含む複数のフィンガープリンティングワードを定義するステップであって、前記フィンガープリンティングワードは各々個々のブロックに配列された複数の拡散シーケンスを含み、前記フィンガープリンティングワードは、関連するフィンガープリンティングワードを変更する潜在的な共謀者の身元を確認する共謀者の解析を可能にするために構築されるステップと、
個々のフィンガープリンティングワードを個々のそれぞれのユーザに割り当てて、前記フィンガープリンティングワードを、それを割り当てられたユーザを識別するのに用いるステップと、
複数のオブジェクトにそれぞれの個々のフィンガープリンティングワードを埋め込んで

個々の被保護オブジェクトを提供するステップと、
前記被保護オブジェクトを個々のユーザに配布するステップと、
被保護オブジェクトを受信するステップと、
前記被保護オブジェクトを充分に処理して、前記受信した被保護オブジェクトに含まれるフィンガープリンティングワードに関連付けられるユーザを識別するステップと
を備え、
前記処理するステップは、
元の拡散シーケンスブロック値の１の補数に対する各ブロックの重みを計算して、各ブロックが可視である可能性が高いか、不可視である可能性が高いかを決定するステップと、
特定の前記ブロックが不可視である可能性が高いと決定されたならば、前記特定のブロックの前記重みを予め定められた値に制限するステップと
を備える、オブジェクトを保護する方法を実行させる命令が記録されたことを特徴とするコンピュータ読み取り可能記録媒体。
【請求項１３】
デジタルデータを含むオブジェクトを保護する方法であって、
各々が少なくとも1つの拡散シーケンス含む複数の一意のフィンガープリンティングワードを定義するステップであって、前記フィンガープリンティングワードは、関連するフィンガープリンティングワードを変更する潜在的な共謀者の身元を確認する共謀者の解析を可能にするために構築され、前記定義するステップは、各フィンガープリンティングワードを同数のΓシンボルを含むように定義するステップを備え、各Γシンボルに２ｃ－１個（ここで、ｃは防御したい共謀者の人数である）の拡散シーケンスを含ませるステップと、
各フィンガープリンティングワードを、潜在的な共謀者を構成することができる個々のユーザに関連付けるステップと、
デジタルデータを含む複数のオブジェクトに個々のフィンガープリンティングワードを埋め込んで被保護オブジェクトを提供するステップと、
前記被保護オブジェクトを前記個々のユーザに配布するステップと
を備えることを特徴とする方法。
【請求項１４】
コンピュータによって実行されたときに請求項１３に記載の方法を実行するコンピュータ実行可能命令をその中に有することを特徴とする1つまたは複数のコンピュータ可読媒体。
【請求項１５】
個々の拡散シーケンスを定義する個々のブロックに配列された複数のスペクトル拡散チップを含むフィンガープリンティングワードをその中に埋め込んだ被保護オブジェクトを受信する手段と、
前記フィンガープリンティングワードに関連付けられる、潜在的な共謀者を含むユーザを識別するのに充分に前記被保護オブジェクトを処理する手段と
を備え、
前記処理する手段は、
元の拡散シーケンスブロック値の１の補数に対する各ブロックの重みを計算して、各ブロックが可視である可能性が高いか、不可視である可能性が高いかを決定する手段と、
特定の前記ブロックが不可視である可能性が高いと決定されたならば、前記特定のブロックの前記重みを予め定められた値に制限する手段と
を備えることを特徴とする、フィンガープリンティングワードを検出するシステム。
【請求項１６】
コンピュータによって実行されたときに請求項１５に記載のシステムを実装するコンピュータ実行可能命令をその中に有することを特徴とするコンピュータ可読媒体。
【請求項１７】

個々の拡散シーケンスを定義する個々のブロックに配列された複数のスペクトル拡散チップを含むフィンガープリンティングワードをその中に埋め込んだ被保護オブジェクトを受信する手段と、
前記フィンガープリンティングワードに関連付けられる、潜在的な共謀者を含むユーザを識別するのに充分に前記被保護オブジェクトを処理する手段と
を備え、
前記処理する手段は、
元の拡散シーケンスブロック値の１の補数に対する各ブロックの重みを計算して、各ブロックが可視である可能性が高いか、不可視である可能性が高いかを決定する手段と、
特定の前記ブロックが不可視である可能性が高いと決定されたならば、前記特定のブロックの前記重みを予め定められた値に制限する手段と
を備える
ことを特徴とする、フィンガープリンティングワードを検出するシステム。
【請求項１８】
コンピュータによって実行されたときに請求項１７に記載のシステムを実装するコンピュータ実行可能命令をその中に有することを特徴とするコンピュータ可読媒体。
【請求項１９】
個々の拡散シーケンスを定義する個々のブロックに配列された複数のスペクトル拡散チップを含むフィンガープリンティングワードをその中に埋め込んだ被保護オブジェクトを受信する手段と、
前記フィンガープリンティングワードに関連付けられる、潜在的な共謀者を含むユーザを識別するのに充分に前記被保護オブジェクトを処理する手段と
を備え、
前記処理する手段は、
元の拡散シーケンスブロック値の１の補数に対する各ブロックの重みを計算して、各ブロックが可視である可能性が高いか、不可視である可能性が高いかを決定する手段と、
特定の前記ブロックが不可視である可能性が高いと決定されたならば、前記特定のブロックの前記重みを予め定められた値に制限する手段と
を備え、
前記予め定められた値は（１－δ）μに等しく、ここで、Ｎ人のユーザの場合、誤り発生確率εでサイズｃの共謀を防御するために、
フィンガープリンティングワード当たりのΓシンボルの数＝Ｌ＝２ｃｌｎ（２Ｎ／ε）
ブロックサイズ(チップで測定)＝ｄ＝８ｃ^{2}ｌｎ（８ｃＬ／ε）
ｆ＝２ｌｎ（４ｃ^{2}ｌｎ（２Ｎ／ε）／ε）
δ＝ｆ／√（ｄ／２）
μ＝ｄ／２
を選択することを特徴とする、フィンガープリンティングワードを検出するシステム。
【請求項２０】
コンピュータによって実行されたときに請求項１９に記載のシステムを実装するコンピュータ実行可能命令をその中に有することを特徴とするコンピュータ可読媒体。
【請求項２１】
各々が一意でありかつ少なくとも1つの拡散シーケンスを含む複数のフィンガープリンティングワードを定義する手段であって、各フィンガープリンティングワードは複数のΓシンボルを含み、各Γシンボルは２ｃ－１個（ここで、ｃは防御したい共謀者の人数である）、の拡散シーケンスを含み、前記フィンガープリンティングワードは、関連するフィンガープリンティングワードを変更する潜在的な共謀者の身元を確認する共謀者解析を可能にするために構築される手段と、
個々のフィンガープリンティングワードを、潜在的な共謀者を構成する個々のそれぞれのユーザに割り当てて、前記フィンガープリンティングワードを、それを割り当てられたユーザを識別するのに用いる手段と

を備えることを特徴とする、Γコードを形成するシステム。
【請求項２２】
各々が一意でありかつ少なくとも1つの拡散シーケンスを含む複数のフィンガープリンティングワードを定義する手段であって、前記フィンガープリンティングワードは関連するフィンガープリンティングワードを変更する潜在的な共謀者を含むユーザの身元を確認する共謀者の解析を可能にするために構成され、前記フィンガープリンティングワードは各々複数の拡散シーケンスを含み、各フィンガープリンティングワードの拡散シーケンスは個々のブロックに配列される手段と、
個々のフィンガープリンティングワードを個々の前記ユーザに割り当てて、前記フィンガープリンティングワードを、それを割り当てられたユーザを識別するのに用いる手段と、
複数のオブジェクトにそれぞれの個々のフィンガープリンティングワードを埋め込んで個々の被保護オブジェクトを提供する手段と、
前記被保護オブジェクトを前記個々のユーザに配布する手段と、
被保護オブジェクトを受信する手段と、
前記被保護オブジェクトを充分に処理して、前記受信した被保護オブジェクトに含まれるフィンガープリンティングワードに関連付けられるユーザを識別する手段と
を備え、
前記処理する手段は、
元の拡散シーケンスブロック値の１の補数に対する各ブロックの重みを計算して、各ブロックが可視である可能性が高いか、不可視である可能性が高いかを決定する手段と、
特定のブロックが不可視である可能性が高いと決定されたならば、前記特定のブロックの前記重みを予め定められた値に制限する手段と
を備えることを特徴とする、オブジェクトを保護するシステム。
【請求項２３】
前記制限する手段は、ブロックが不可視である可能性が高い場合にそうする手段を備えることを特徴とする、請求項２２に記載のシステム。
【請求項２４】
前記予め定められた値は（１－δ）μに等しく、ここで、Ｎ人のユーザの場合、誤り発生確率εでサイズｃの共謀を防御するために、
フィンガープリンティングワード当たりのΓシンボルの数＝Ｌ＝２ｃｌｎ（２Ｎ／ε）
ブロックサイズ(チップで測定)＝ｄ＝８ｃ^{2}ｌｎ（８ｃＬ／ε）
ｆ＝２ｌｎ（４ｃ^{2}ｌｎ（２Ｎ／ε）／ε）
δ＝ｆ／√（ｄ／２）
μ＝ｄ／２
を選択することを特徴とする、請求項２２に記載のシステム。
【請求項２５】
前記埋め込まれたフィンガープリンティングワードは、各々複数のブロック含む複数のΓシンボルを有し、複数のユーザの各々は複数のΓシンボルを有する一意のフィンガープリンティングワードを割り当てられ、
前記処理する手段は、
前記埋め込まれたフィンガープリンティングワードの各Γシンボルについて、共謀の対象である可能性のある1つまたは複数の色のセットを決定する手段と、
前記ユーザのフィンガープリンティングワードの各々について、各Γシンボルを評価して、それが、前記埋め込まれたフィンガープリンティングワードの対応するΓシンボルのセット内の色と一致するか否かを確認する手段と、
最大数の色を有するユーザを選択する手段と
を備えることを特徴とする、請求項２２に記載のシステム。
【請求項２６】
一意でありかつ少なくとも１つの拡散シーケンスを含む複数のフィンガープリンティン

グワードを定義する手段であって、前記フィンガープリンティングワードは関連するフィンガープリンティングワードを変更する潜在的な共謀者の身元を確認する共謀者解析を可能にするために構成され、前記定義は複数のΓシンボルを含むように各フィンガープリンティングワードを定義することを備え、各Γシンボルは複数の拡散シーケンスを含み、各フィンガープリンティングワードは同数のΓシンボルを含み、各Γシンボルは２ｃ－１個（ここで、cは防御したい共謀者の人数である）の拡散シーケンスを含む手段と、

各フィンガープリンティングワードを潜在的な共謀者を構成する場合がある個々のユーザと関連付ける手段と、

デジタルデータを含む複数のオブジェクトに個々のフィンガープリンティングワードを埋め込んで被保護オブジェクトを提供する手段と、

前記被保護オブジェクトを前記個々のユーザに配布する手段と

を備えることを特徴とする、デジタルデータを含むオブジェクトを保護するシステム。

【請求項２７】

各々が一意でありかっ少なくとも1つの拡散シーケンスを含む複数のフィンガープリンティングワードを定義する手段であって、前記フィンガープリンティングワードは関連するフィンガープリンティングワードを変更する潜在的な共謀者を含むユーザの身元を確認する共謀者解析を可能にするために構成され、前記フィンガープリンティングワードは各々複数の拡散シーケンスを含み、各フィンガープリンティングワードの前記拡散シーケンスは個々のブロックに配列される手段と、

個々のフィンガープリンティングワードを個々のそれぞれの前記ユーザに割り当てて、前記フィンガーブリンティングワードを、それを割り当てられたユーザを識別するのに用いる手段と、

複数のオブジェクトにそれぞれの個々のフィンガープリンティングワードを埋め込んで個々の被保護オブジェクトを提供する手段と、

前記被保護オブジェクトを前記個々のユーザに配布する手段と、

被保護オブジェクトを受信する手段と、

前記被保護オブジェクトを充分に処理して、前記受信した被保護オブジェクトに含まれるフィンガープリンティングワードに関連付けられるユーザを識別する手段と

を備え、

前記処理する手段は、

元の拡散シーケンスブロック値の１の補数に対する各ブロックの重みを計算して、各ブロックが可視である可能性が高いか、不可視である可能性が高いかを決定する手段と、

特定の前記ブロックが不可視である可能性が高いと決定されたならば、前記特定のブロックの前記重みを予め定められた値に制限する手段と

を備え、

前記予め定められた値は（１－δ）μに等しく、ここで、Ｎ人のユーザの場合、誤り発生確率εでサイズｃの共謀を防御するために、

フィンガープリンティングワード当たりのΓシンボルの数＝Ｌ＝２ｃｌｎ（２Ｎ／ε）

ブロックサイズ(チップで測定)＝ｄ＝８ｃ^{2}ｌｎ（８ｃＬ／ε）

ｆ＝２ｌｎ（４ｃ^{2}ｌｎ（２Ｎ／ε）／ε）

δ＝ｆ／√（ｄ／２）

μ＝ｄ／２

を選択することを特徴とする、オブジェクトを保護するシステム。

【請求項２８】

各々が一意でありかつ少なくとも1つの拡散シーケンスを含む複数のフィンガープリンティングワードを定義する手段であって、前記フィンガープリンティングワードは関連するフィンガープリンティングワードを変更する潜在的な共謀者を含むユーザの身元を確認する共謀者解析を可能にするために構成され、前記フィンガープリンティングワードは各々複数の拡散シーケンスを含み、各フィンガープリンティングワードの前記拡散シーケンス定義は個々のブロックに配列される手段と、

個々のフィンガープリンティングワードを個々のそれぞれの前記ユーザに割り当てて、前記フィンガープリンティングワードを、それを割り当てられたユーザを識別するのに用いる手段と、
複数のオブジェクトにそれぞれの個々のフィンガープリンティングワードを埋め込んで個々の被保護オブジェクトを提供する手段と、
前記被保護オブジェクトを前記個々のユーザに配布する手段と、
被保護オブジェクトを受信する手段と、
前記被保護オブジェクトを充分に処理して、前記受信した被保護オブジェクトに含まれるフィンガープリンティングワードに関連付けられるユーザを識別する手段と
を備え、
前記処理する手段は、
元の拡散シーケンスブロック値の１の補数に対する各ブロックの重みを計算して、各ブロックが可視である可能性が高いか、不可視である可能性が高いかを決定する手段と、
特定の前記ブロックが不可視である可能性が高いと決定されたならば、前記特定のブロックの前記重みを予め定められた値に制限する手段と
を備えることを特徴とする、オブジェクトを保護するシステム。
【請求項２９】
デジタルデータを含むオブジェクトを保護するためにコンピュータによって実施される方法であって、
複数の一意のフィンガープリンティングワードを構築して、関連するフィンガープリンティングワードを変更する潜在的な共謀者の身元を確認する共謀者の解析を可能にするステップであって、前記フィンガープリンティングワードからコードテーブルが定義され、前記コードテーブルの各行は前記フィンガープリンティングワードの個々の1つを含み、各フィンガープリンティングワードは複数のブロックにセグメント化され、各ブロックは前記コードテーブルの他のフィンガープリンティングワードの対応するブロックと連動して前記コードテーブルの列を定義し、各フィンガープリンティングワードの少なくとも１つのブロックが拡散シーケンスを含むステップと、
前記コードテーブル内の各フィンガープリンティングワードを、潜在的な共謀者を構成するそれぞれのユーザと関連付けて、個々のフィンガープリンティングワードを、それが割り当てられたユーザを識別するのに用いるステップと、
前記コードテーブルの列を並べ替えるステップと、
デジタルデータを含む複数のオブジェクトの各々に、前記並び替えられたコードテーブルにより定義されたそれぞれの個々のフィンガープリンティングワードを埋め込んで被保護オブジェクトを提供するステップと
を備えることを特徴とする方法。
【請求項３０】
各フィンガープリンティングワードが複数のΓシンボルを含み、Γシンボルは複数の前記ブロックを含み、各Γシンボルは少なくとも1つの拡散シーケンスを含むことを特徴とする、請求項２９に記載の方法。
【請求項３１】
各Γシンボルは複数の拡散シーケンスを含むことを特徴とする、請求項３０に記載の方法。
【請求項３２】
各フィンガープリンティングワードは同数のΓシンボルを含むことを特徴とする、請求項３１に記載の方法。
【請求項３３】
各Γシンボルは２ｃ－１個の拡散シーケンスを含み、ここでｃは防御したい共謀者の人数であることを特徴とする、請求項３０～３２のうちのいずれか１つに記載の方法。
【請求項３４】
前記複数のプリンティングワードを定義するステップは、前記フィンガープリンティン

グワードの長さを選択するステップを備え、前記長さは防御したい共謀者の人数と誤り発生率（ε）の関数であることを特徴とする、請求項２９～３３のうちのいずれか１つに記載の方法。

【請求項３５】

前記被保護オブジェクトを個々のユーザに配布するステップをさらに備えることを特徴とする、請求項２９～３４のうちのいずれか１つに記載の方法。

【請求項３６】

前記列を並び替えるステップは、前記コードテーブル内の拡散シーケンスのチップをランダムに混ぜることにより実行されることを特徴とする、請求項２９～３５のうちののいずれか１つに記載の方法。

【請求項３７】

フィンガープリンティングワードを検出するためにコンピュータによって実施される方法であって、

複数の個々のブロックを含むフィンガープリンティングワードであって、少なくとも1つの前記ブロックが個々の拡散シーケンスを含むフィンガープリンティングワードを埋め込んだ被保護オブジェクトを受信するステップと、

前記フィンガープリンティングワードに関連付けられた被保護オブジェクトを処理するステップと

を備え、

前記フィンガープリンティングワードは行および列を有するコードテーブル、即ちΓコードを定義することにより定義され、前記行はそれぞれ1つのフィンガープリンティングワードを定義し、前記列は前記コードテーブル内の各フィンガープリンティングワードの対応するブロックにより形成され、前記フィンガープリンティングワードは前記コードテーブルの列を並び替えることによりさらに定義され、

前記被保護オブジェクトを処理するステップは、

前記埋め込まれたフィンガープリンティングワードの列の並び替えを解除するステップと、

個々の拡散シーケンスを含む少なくとも1つの個々のブロックを含む、前記並び替えが解除されかつ埋め込まれたフィンガープリンティングワードのブロックを評価するステップと、

元の拡散シーケンスブロック値の１の補数に対する各ブロックの重みを決定し、各ブロックが可視である可能性が高いか、不可視である可能性が高いかを決定するステップと

を備えることを特徴とする方法。

【請求項３８】

前記処理するステップは、特定のブロックが不可視である可能性が高いと決定されたならば、前記特定のブロックの重さを所定の値に制限するステップをさらに備えることを特徴とする、請求項３７に記載の方法。

【請求項３９】

前記制限するステップは、ブロックが潜在的な共謀者により見られる可能性が高い場合にそうすることを特徴とする、請求項３８に記載の方法。

【請求項４０】

前記予め定められた値は（１－δ）μに等しく、ここで、Ｎ人のユーザの場合、誤り発生確率εでサイズｃの共謀を防御するために、

フィンガープリンティングワード当たりのΓシンボルの数＝Ｌ＝２ｃｌｎ（２Ｎ／ε）

ブロックサイズ(チップで測定)＝ｄ＝８ｃ^{2}ｌｎ（８ｃＬ／ε）

ｆ＝２ｌｎ（４ｃ^{2}ｌｎ（２Ｎ／ε）／ε）

δ＝ｆ／√（ｄ／２）

μ＝ｄ／２

を選択することを特徴とする、請求項３８に記載の方法。

【請求項４１】

前記埋め込まれたフィンガープリンティングワードは、各々が複数のブロックを含む複数のΓシンボルを有し、複数のオブジェクトのそれぞれには、複数のΓシンボルを有する一意のフィンガープリンティングワードが割り当てられ、
前記処理するステップは、
前記埋め込まれたフィンガープリンティングワードの各Γシンボルについて、共謀の対象である可能性のある1つまたは複数の色のセットを決定するステップと、
前記フィンガープリンティングワードの各々について、各Γシンボルを評価して、前記埋め込まれたフィンガープリンティングワードの対応するΓシンボルのセット内の色と一致するかを確認するステップと、
最大数の色を有するオブジェクトを選択するステップと
を備えることを特徴とする、請求項３８に記載の方法。
【請求項４２】
前記決定するステップは、
各ブロックの重みを評価するステップと、
前記ブロックの重みが予め定められた関係を満たす場合、Γシンボルを選択するステップと
を備えることを特徴とする、請求項４１に記載の方法。
【請求項４３】
前記Γコードは複数の拡散シーケンスを含むデータ構造であり、
前記拡散シーケンスは、被保護オブジェクトが分配される個々のユーザに割り当て可能なフィンガープリンティングワードを定義するために結合可能なブロックに配列されることを特徴とする、請求項２９～４２のうちののいずれか１つに記載の方法。
【請求項４４】
コンピュータによって実行されたときに、請求項２９～４３のうちのいずれか１つに記載の方法を実行するコンピュータ実行可能命令を記録したことを特徴とするコンピュータ可読媒体。
【発明の詳細な説明】
【０００１】
（技術分野）
本発明は、デジタルデータのフィンガープリンティング（ｆｉｎｇｅｒｐｒｉｎｔｉｎｇ）のための方法およびシステムに関する。
【０００２】
（発明の背景）
フィンガープリンティングは、特定のオブジェクトの各コピーに一意のマーク付けを行うこと、および一意のマーク付けが行われた各コピーに、そのコピーが配布される特定のエンティティを関連付けることを含む技術である。一意にマーク付けされたコピーの無許可コピーが作成された場合、コピーが最初に配布された元のエンティティまでフィンガープリントを追跡することができる。
【０００３】
一例として、印刷された地図について考察する。地図製作者が地図を作成するときに、彼らは、地図を配布された個人が地図の無許可コピーを作成してそれを他人に配布しないという保証を欲するであろう。地図製作者が彼の地図を保護する１つの方法は、配布される地図のコピーの各々に異なる些細な誤りまたはフィンガープリント（例えば存在しない街路）を導入することである。次いで各フィンガープリントにマップが配布される個人を関連付ける。各フィンガープリントに異なる個人を関連付けることによって、その個人のコピーの無許可コピーが明らかになった場合に、その地図に含まれる一意のフィンガープリントによって、それらを元の個人まで追跡することができる。
【０００４】
この種のフィンガープリンティングの１つの問題は、２人または３人以上の個人が彼らのフィンガープリントを発見する目的のために共謀するときに発生することがあり得る。つ

まり、２人またはそれ以上の個人が集まって、彼らの地図を比較すると、彼らは、充分な時間があれば、単に彼らの地図間の相違を探すだけで、彼らの一意のフィンガープリントを突き止めることができる。彼らが自分のフィンガープリントを突き止めることができれば、彼らはそれを変更することができ、したがっておそらく検出を回避することができる。

【０００５】

現代において、特にインターネットおよび電子配信の登場により、無許可コピーを検出または抑止するために、デジタルデータ（例えば、ソフトウェア、文書、音楽、映像）にフィンガープリンティングを施すことが重要になってきた。上記の地図の例と同様に、デジタル文脈で異なる個人による共謀が、そのようなデジタルデータの所有者および配布者に対する挑戦をもたらすおそれがある。デジタルフィンガープリンティングの領域は進歩してきたが、デジタルフィンガープリンティングによってもたらされる保護の幅を広げるために、さらなる進展が必要である。例えば、あるフィンガープリンティングシステム（以下で詳述する「Ｂｏｎｅｈ－Ｓｈａｗ」システム）では、共謀に対する多少の防御が提供されるが、共謀者の人数が比較的少ない場合に限られる。そこで、デジタルフィンガープリンティングによって提供される保護を増強して、共謀者の人数が多い場合でも共謀者を検出する必要がある。

【０００６】

したがって、本発明は、デジタルデータのフィンガープリンティングのための改善された方法およびシステムを提供することに関連する関心から生まれたものである。

【０００７】

（発明の概要）

デジタルデータのフィンガープリンティングのための方法およびシステムについて記載する。記載する実施形態では、直接拡散式スペクトル拡散（ＤＳＳＳ）技術を利用する。各々に少なくとも１つの拡散シーケンスが含まれる、一意のフィンガープリンティングワードを定義する。記載する実施形態では、フィンガープリンティングワードは「Γシンボル」と呼ばれる複数のシンボルを含む。各Γシンボルは２ｃ－１個のブロックから成る。ここでｃは防御したい共謀者の人数を表わす。各ブロックはｄ個の拡散シーケンスチップを含む。フィンガープリンティングワードは、フィンガープリンティングワードを埋め込まれた被保護オブジェクトが配布される複数のエンティティに割り当てられる。

【０００８】

その一意のフィンガープリンティングワードを改ざんしたエンティティの身元を突き止めるために、定義された関数に従って各ブロックの相対重みが計算され、重みが予め定められた関係を満たすブロックは、いわゆる作業範囲に「クリップ（ｃｌｉｐｐｅｄ）」される。次いで、改ざんされたフィンガープリンティングワードの各Γシンボルが処理されて、共謀の対象（サブジェクト）であるかもしれない１つまたは複数の「色」のセットが生成される。次いで、各エンティティのフィンガープリンティングワード内の各Γシンボルが、対応する生成されたセットに照らして評価され、最も多くの全般的に有罪を示す「色」を有するエンティティが有罪として示される。

【０００９】

（好適な実施形態の詳細な説明）

概要

記載する実施形態では、デジタルデータまたはオブジェクトに一意のフィンガープリンティングワードがフィンガープリントされる。すなわち、埋め込まれる。各フィンガープリンティングワードは、フィンガープリンティングを施したオブジェクトが配布される多数のエンティティの１つまたは多数のユーザの１人に関連付けられる。記載する方式では、各フィンガープリンティングワードは複数のΓシンボルを含み、各Γシンボルは複数のブロックを含む。各ブロックは次に、複数の拡散シーケンスチップを有する拡散シーケンスを含む。

【００１０】

改ざんされたオブジェクトを受信すると、それは最初に、埋め込まれた拡散シーケンスチップを識別するために処理される。ひとたびチップが識別されると、相対重み関数が定義され、各ブロックの相対重みを計算するために使用される。各ブロックの相対重み計算は、ブロックのうちのどれを予め定義された作業範囲に「クリップ」させるかを決定する、予め定められた関係に従って分析される。クリップされたブロックは、改ざんされたオブジェクトを生成するために共謀した共謀者がおそらくこれらのブロックを見ることができなかったという意味で、「目に見えない（ｕｎｓｅｅｎ）」と思われるブロックである。すなわち、それらは変わっていない。クリップされないブロックは、おそらく「目に見え（ｓｅｅｎ）」、したがって共謀者によっておそらく改ざんされたと思われるブロックを構成する。

【００１１】

計算された各ブロックの相対重みおよび定義された作業範囲により、改ざんされたオブジェクトの各Γシンボルが処理され、共謀の対象であるかもしれない可能性のあるΓシンボルのセットが生成される。セットの集合がマトリックスを画定する。次いで、ユーザの一意のフィンガープリントの各Γシンボルが、マトリックス内の各々の対応するΓシンボルのセットと比較され、各ユーザのΓシンボルが特定のセット内で見つかったΓシンボルと一致する回数が計数される。全てのユーザをこうして評価し終わったときに、最も高い計数のユーザが、改ざんされたオブジェクトを生成した共謀者として選択される。

【００１２】

例示的コンピュータシステム

図１は、本発明に従って使用することができるコンピュータ１３０の一般例である。分散コンピューティング環境の文脈で、図示するような様々な数のコンピュータを使用することができる。

【００１３】

コンピュータ１３０は、１つまたは複数のプロセッサまたは処理装置１３２と、システムメモリ１３４と、システムメモリ１３４をはじめ様々なシステム構成要素をプロセッサ１３２につなぐバス１３６とを含む。バス１３６は、メモリバスまたはメモリコントローラ、周辺バス、アクセラレーテッドグラフィックスポート（ａｃｃｅｌｅｒａｔｅｄ　ｇｒａｐｈｉｃｓ　ｐｏｒｔ）、および多種多様なバスアーキテクチャのいずれかを使用するプロセッサまたはローカルバスをはじめ、数種類ある中のいずれかのバス構造の１つまたは複数を表わす。システムメモリ１３４は、読出し専用メモリ（ＲＯＭ）１３８およびランダムアクセスメモリ（ＲＡＭ）１４０を含む。起動中などにコンピュータ１３０内の要素間で情報を転送するのに役立つ基本ルーチンを含む、基本入力／出力システム（ＢＩＯＳ）１４２はＲＯＭ１３８に格納される。

【００１４】

コンピュータ１３０は、ハードディスク（図示せず）からの読出しおよびそこへの書込みのためのハードディスクドライブ１４４、取外し可能磁気ディスク１４８からの読出しおよびそこへの書込みのための磁気ディスクドライブ１４６、およびＣＤ　ＲＯＭまたは他の光媒体などの取外し可能光ディスク１５２からの読出しおよびそこへの書込みのための光ディスクドライブ１５０をさらに含む。ハードディスクドライブ１４４、磁気ディスクドライブ１４６、および光ディスクドライブ１５０は、ＳＣＳＩインタフェース１５４または他の適切なインタフェースによってバス１３６に接続される。ドライブおよびそれらの関連するコンピュータ読出し可能な媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、およびコンピュータ１３０のためのその他のデータの不揮発性記憶装置を提供する。ここで記載する例示的環境はハードディスク、取外し可能ディスク１４８、および取外し可能光ディスク１５２を使用しているが、磁気カセット、フラッシュメモリカード、デジタルビデオディスク、ランダムアクセスメモリ（ＲＡＭ）、読出し専用メモリ（ＲＯＭ）など、コンピュータによってアクセス可能なデータを格納できる、他の種類のコンピュータ可読媒体を例示的動作環境で使用することもできることを、当業者は理解されたい。

【００１５】
オペレーティングシステム１５８、１つまたは複数のアプリケーションプログラム１６０、他のプログラムモジュール１６２、およびプログラムデータ１６４を含む多数のプログラムモジュールを、ハードディスク１４４、磁気ディスク１４８、光ディスク１５２、ＲＯＭ１３８、またはＲＡＭ１４０に格納することができる。ユーザは、キーボード１６６およびポインティング装置１６８などの入力装置を通して、コマンドおよび情報をコンピュータ１３０に入力することができる。他の入力装置（図示せず）として、マイクロホン、ジョイスティック、ゲームパッド、衛星放送受信アンテナ（ｓａｔｅｌｌｉｔｅ ｄｉｓｈ）、スキャナなどを含めることができる。これらおよびその他の入力装置は、バス１３６に結合されたインタフェース１７０を介して処理装置１３２に接続される。ビデオアダプタ１７４などのインタフェースを介して、モニタ１７２またはその他の種類の表示装置もまたバス１３６に接続される。モニタに加えて、パーソナルコンピュータは一般的に、スピーカおよびプリンタなどの、他の周辺出力装置（図示せず）を含む。

【００１６】
コンピュータ１３０は一般的に、遠隔コンピュータ１７６など、１つまたは複数の遠隔コンピュータへの論理接続を使用するネットワーク環境で作動する。遠隔コンピュータ１７６は別のパーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピアデバイス（ｐｅｅｒ ｄｅｖｉｃｅ）または他の一般的ネットワークノードとすることができ、一般的に、コンピュータ１３０に関連して上述した要素の多くまたは全部を含むが、図１には記憶装置１７８しか図示されていない。図１に示された論理接続は、ローカルエリアネットワーク（ＬＡＮ）１８０および広域ネットワーク（ＷＡＮ）１８２を含む。そのようなネットワーク環境はオフィス、企業内コンピュータネットワーク、イントラネット、およびインターネットで一般的である。

【００１７】
ＬＡＮネットワーク環境で使用する場合、コンピュータ１３０は、ネットワークインタフェースまたはアダプタ１８４を通してローカルネットワーク１８０に接続される。ＷＡＮネットワーク環境で使用する場合、コンピュータ１３０は一般的にモデム１８６、またはインターネットなど広域ネットワーク１８２で通信を確立するための他の手段を含む。内蔵または外付けとすることのできるモデム１８６は、シリアルポートインタフェース１５６を介してバス１３６に接続される。ネットワーク環境では、パーソナルコンピュータ１３０に関連して示したプログラムモジュールまたはその一部を遠隔記憶装置内に格納することができる。図示したネットワーク接続は例示であり、コンピュータ間に通信リンクを確立する他の手段を使用することができることは理解されるであろう。

【００１８】
一般的に、コンピュータ１３０のデータプロセッサは、様々な時期にコンピュータの様々なコンピュータ可読記憶媒体に格納された命令によってプログラムされる。プログラムおよびオペレーティングシステムは一般的に、例えばフロッピー（登録商標）ディスクまたはＣＤ－ＲＯＭで配布される。そこから、それらはコンピュータの二次メモリ内にインストールまたはロードされる。実行時に、それらは少なくとも部分的にコンピュータの一次電子メモリ内にロードされる。これらおよびその他の様々な種類のコンピュータ可読記憶媒体が、マイクロプロセッサまたは他のデータプロセッサに関連して以下で説明するステップを実現するための命令またはプログラムを含む場合、ここで記載する発明は、そのような媒体を含む。本発明はまた、以下で説明する方法および技術に従ってプログラムされる場合、コンピュータ自体をも含む。

【００１９】
例証のために、オペレーティングシステムなどのプログラムおよび他の実行可能なプログラム構成要素は、ここでは離散ブロックとして図示するが、そのようなプログラムおよび構成要素は様々な時期にコンピュータの様々な記憶装置構成要素に常駐し、コンピュータのデータプロセッサによって実行されることを理解されたい。

【００２０】

Ｂｏｎｅｈ－Ｓｈａｗシステム
Ｂｏｎｅｈ－Ｓｈａｗシステム（以下「ＢＳシステム」）は、デジタルデータ用のフィンガープリンティングシステムである。ＢＳシステムは、デジタルデータにフィンガープリンティングを行うときに、共謀の問題を克服しようと試みるものである。ＢＳシステムの態様は、ＩＥＥＥ Ｔｒａｎｓａｃｔｉｏｎｓ ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｔｈｅｏｒｙ、Ｖｏｌ．４４、Ｎｏ．５、Ｓｅｐｔｅｍｂｅｒ １９９８に掲載された、ＢｏｎｅｈおよびＳｈａｗによる「Ｃｏｌｌｕｓｉｏｎ－Ｓｅｃｕｒｅ Ｆｉｎｇｅｒｐｒｉｎｔｉｎｇ ｆｏｒ Ｄｉｇｉｔａｌ Ｄａｔａ」と題する論文に記載されている。
【００２１】
ＢＳシステムの原理仮定の１つは、「マーク付け仮定（ｍａｒｋｉｎｇ ａｓｓｕｍｐｔｉｏｎ）」として知られている。すなわち、ユーザは、どのデータにマークが含まれるかを決定することができなければ、マークを改ざんできない、というものである。オブジェクトにフィンガープリンティングが行われるときに、各エンティティまたはユーザに一意のフィンガープリンティングワードがオブジェクトに埋め込まれる。ユーザは共謀することによって、彼らのコピーの間で特定のマークが異なっている場合に、そのマークを検出することができる。異なっていなければ、マークは検出できない。これがマーク付け仮定の基本である。すなわち、彼らは見ることのできないマークを変更することはできない。これらのマークは、「不可視」マークと呼ばれる。
【００２２】
ＢＳシステムでは、各ユーザに一意のフィンガープリンティングワードが割り当てられる。フィンガープリンティングワードの割当ての一例を、５人のユーザの場合について図２に示す。各行はユーザに対応し、そのユーザのフィンガープリンティングワードを形成するブロックを示す。例えば、ユーザ１はフィンガープリンティングワード「１１１１１１１１１１１１１１１１」を持ち、ユーザ２はフィンガープリンティングワード「０００００１１１１１１１１１１１１１１」を持ち、各々のユーザについて以下同様に続く。全てのユーザのフィンガープリンティングワードの集合は、表中の太線によって示される階段構造を定義する。この階段状構造は、以下で明らかになるように、潜在的な共謀者を突き止めるのに役立つ。
【００２３】
各フィンガープリンティングワードは、今度は複数のビットを含む多数のブロックに分割される。この例では、ブロック０、ブロック１、ブロック２、およびブロック３と指定された４つのブロックがある。各々のブロックが、この例では４ビットを含む。この考察を目的として、フィンガープリンティングワードの割当てによって画定されるマトリックスは「Γコード」として知られる。非常に多くのユーザがいる場合、全てのユーザにフィンガープリンティングワードを提供するために必要なΓコードは極めて大きくなる。
【００２４】
ＢＳシステムによると、オブジェクトにフィンガープリンティングワードを埋め込む前に、Γコードの列の１回の並べ替えが行われる。ブロックの順序が変更される例示的並べ替えを下の表１に示す。説明を簡単にするため、上の表に該当する並べ替えは、ブロック全体に行われている。実際には並べ替えはビットレベルで行われる。例えば、左端のビットの列は、ビット位置１２に移される可能性がある。この並べ替えは全てのユーザに対して一様であり、符号器または埋込み器および復号器だけに知らされる。
【００２５】
【表１】

ユーザ	ブロック２	ブロック１	ブロック３	ブロック０
1	1111	1111	1111	1111
2	1111	1111	1111	0000
3	1111	0000	1111	0000
4	0000	0000	1111	0000
5	0000	0000	0000	0000

表１

【００２６】
オブジェクトにフィンガープリンティングを行う場合、ユーザの１人に対応する並べ替えられたフィンガープリンティングワードがそれに埋め込まれる。考察を目的として、「オブジェクト」とはフィンガープリンティングに適した任意のデジタルデータである。そのようなオブジェクトの例は、文書、音楽、および映像を含むが、これらに限定されない。被保護オブジェクトの不正コピーが行われる場合、ユーザは一般的に、検出を回避するために彼らのフィンガープリンティングワードを改ざんしようとする。ＢＳシステムは、被保護オブジェクトの改ざんに協力したかもしれない１人またはそれ以上のユーザの身元を、所望の程度の確実さで、突き止めることに向けられている。これは、改ざんされたオブジェクトを調べることによって行われる。

【００２７】
以下の考察では、改ざんされたオブジェクトをｘで表わす。ここでｘは長さｕのバイナリワードであり、Ｉ＝｛i_1．．．i_r｝はｘのビット位置のサブセット、すなわちＩ⊆｛１．．．ｎ｝である。表記ｘ↓Ｉは、ワードｘがＩのビット位置に制約されることを表わす。Ｗ（ｘ）は文字列ｘのハミング重みを表わす。１および０のバイナリ文字列のハミング重みは、文字列中の１の個数である。同様に、文字列が＋１と－１とから構成される場合、それを文字列中の＋１の個数と定義することができる。

【００２８】
第１アルゴリズム
ＢＳシステムは、改ざんされたオブジェクトｘを生成した結託のサブセットを見つけることに向けられた第１アルゴリズムを使用する。したがって、この時点で、改ざんされたオブジェクトは２人または３人以上のユーザによって生成されたものであり、オブジェクトｘを生成した可能性のあるユーザのサブセットを識別しようとする試みが行われる。見込みのあるユーザ候補のサブセットを生成するアルゴリズムについて述べる前に、次のことを考慮する。改ざんされたオブジェクトｘを受信したとき、それは必然的に何らかの形のフィンガープリンティングワードを含む。一例を上の表１に示した、一意の並べ替えられたフィンガープリンティングワードが、各ユーザに割り当てられていることを思い出されたい。各ユーザに一意のフィンガープリンティングワードが割り当てられるので、フィンガープリンティングワードの特定の態様は、各ユーザに一意である。例えば、図２におけるユーザ１のフィンガープリンティングワードの一意の態様は、ブロック０が全部１からなることである。他のユーザは各々、彼らの対応するブロック０に全部０を含む。したがって、ユーザ１以外のユーザが共謀者である場合には、（ユーザは「不可視」ビットを変更できないという）マーク付け仮定に従って、ブロック０のビットはどれも変更されない。したがって、ブロック０のビットは全て０であり、ユーザ１は共謀者から除外することができる。他方、改ざんされたオブジェクトｘのブロック０のビットのいずれかが１であることが決定された場合には、ユーザ１は共謀者として有罪であることが示される。再びこれは、ブロック０のビットが、他のユーザ全員のブロック０のビットとは異なるので、ユーザ１を含む共謀によってのみ「見る」ことができるからである。こうして、第１アルゴリズムは改ざんされたオブジェクトのフィンガープリンティングワードを単に見て、特定のビットまたはブロックが変更されていることを前提として、どのユーザが有罪の可能

性のある候補者であるかを、所望の程度の確実さで識別しようと試みる。それは、特定のユーザによって一意に見られるか、あるいは見ることのできる特定のブロックのハミング重みを考慮することによって、これを行う。

【００２９】

より具体的な例として、ユーザ３および４が共謀して、彼らの被保護オブジェクトのフィンガープリンティングワードを変更しようとしていると考える。したがってユーザ３および４は、彼らの並び替えられたフィンガープリンティングワードを比較する。上の表１から、この比較は次の通りである。

【００３０】

【表２】

ユーザ	ブロック２	ブロック１	ブロック３	ブロック０
3	1111	0000	1111	0000
4	0000	0000	1111	0000

【００３１】

ユーザ３および４が彼らのフィンガープリンティングワードを比較するときに、ブロック１、３、および０に現われるビットはユーザには「見えない」。これは、それらが同じ値を含むからである。したがって、マーク付け仮定に従って、ユーザはこれらの位置のいずれのビットの値も変更できない。しかし、ブロック２に現われるビットはユーザ間で異なる。すなわち、それらは「見える」。したがって、ユーザ２および３は、この違いのため、ブロック２にフィンガープリントがあるはずだと認識する。これを知って、彼らは次に、検出を回避するようにブロック２のフィンガープリントを変更することができる。この例では、結果的に得られるフィンガープリンティングワードは、このように見えるかもしれない。

【００３２】

【表３】

ユーザ	ブロック２	ブロック１	ブロック３	ブロック０
3	0011	0000	1111	0000
4	0011	0000	1111	0000

【００３３】

ここで、彼らはブロック２の最初の２ビットを「１」から「０」に変更した。彼らは、ブロック２のビットを全部変更すると、結果的に得られるフィンガープリンティングワードがユーザ４のそれと同じになり、ユーザ４が共謀者として有罪になるので、全部は変更しないことに注意されたい。ブロックが並び替えを解除されると、結果的に得られるΓコードはこのように見える。

【００３４】

【表４】

ユーザ	ブロック０	ブロック１	ブロック２	ブロック３
1	1111	1111	1111	1111
2	0000	1111	1111	1111
3	0000	0000	0011	1111
4	0000	0000	0011	1111
5	0000	0000	0000	0000

【００３５】
読者が気付くであろう１つの事は、ユーザ３に対しブロック１および２によって定義されたステップ関数との多少の類似が依然としてあることである。このステップ関数は、上で指摘した通り、ブロック１および２の位置でユーザ３に一意である。すなわち、他のユーザは全員、ユーザ３の上または下のどちらでも、彼らのブロック１および２がそれぞれ全部１または全部０である。
【００３６】
第１アルゴリズムが行うことは、列が並べ替えを解除された後で、最初と最後のユーザ以外のユーザに対するこの一意のステップ関数またはそれに多少類似したものを探すことである。最初と最後のユーザについては、アルゴリズムは単に、最初と最後のユーザに一意のブロック内の一意のビットを探すだけである。ステップ関数（または一意のビット）が突き止められると、対応するユーザを有罪とすることができる。この例では、依然としてユーザ３に対してステップ関数が存在するので、ユーザ３を有罪とすることができる。これは数学的に次のように表わすことができる（εは有罪判定誤り発生確率である）。
【００３７】
アルゴリズム１
１．Ｗ（ｘ↓ブロック１）＞０ならば、ユーザ１は有罪である。
２．Ｗ（ｘ↓ブロック（ｎ－１））＜ｄならば、ユーザｎは有罪である。
３．全てのｓ＝２ないしｎ－１について、
R_s＝（B_{s-1} ∪ B_s）（すなわちこれらの２つの隣接するブロックのビット位置）とする。
Ｋ＝Ｗ（ｘ↓R_s）とする。
Ｗ（ｘ↓ブロック（ｓ－１））＜Ｋ／２－（（Ｋ／２）ｌｏｇ（２ｎ／ε））$^{1/2}$ならば、ユーザ「ｓ」は有罪である。
【００３８】
第２アルゴリズム
上で指摘した通り、任意の被保護オブジェクトの潜在的ユーザの数は極めて大きくなり得る。したがって、上述のΓコード方式を使用すると、結果的にフィンガープリンティングワードは非常に大きいサイズとなる。ＢＳシステムの第２アルゴリズムは、そのような大きいΓコードを使用することを必要とせずに、ユーザまたは共謀者を有罪として示すことに向けられる。このアルゴリズムを使用する場合、ｃは防御したい共謀者の人数を表わす。次いでΓコードは２ｃ行を有するように選択される。このシステムでは、各行が「色」とも呼ばれる。したがって、例えば２０人の共謀者から防御したい場合には、４０の行または色を有するΓコードが選択される。Γコードにおける各行または色は、Γシンボルを形成する複数のブロックを含む。各色またはΓシンボルは、Γコードによって定義されるアルファベットの文字として取り扱われる。次いで、アルファベットの文字は、被保護オブジェクトのユーザの各々に一意のフィンガープリンティングワードを作成するために使用される。すなわち、フィンガープリンティングワードはＬ個の色またはΓシンボルを含む。ここでＬは、フィンガープリンティングワードを割り当てられるユーザの数が与えられた場合に、各人に一意のフィンガープリンティングワードが割り当てられることを保証するのに充分大きくなるように選択される数字である。

【００３９】
一例として、次のように考える。常時、３人の共謀者に対して防御することを希望すると仮定する。したがって、Γコードは２（３）＝６つの色またはΓシンボルを有すると定義される。これを下の表２に示す。
【００４０】
【表５】

色	Γシンボル
1	Γ_1
2	Γ_2
3	Γ_3
4	Γ_4
5	Γ_5
6	Γ_6

表２

【００４１】
さらに、この例では、ユーザの母集団（ｕｎｉｖｅｒｓｅ　ｏｆ　ｕｓｅｒｓ）において、一意のフィンガープリンティングワードが割り当てられる各ユーザに必要なΓシンボルの数は３であると考える。すなわちＬ＝３である。したがって、ユーザ１にはフィンガープリンティングワード（$\Gamma_4\Gamma_5\Gamma_3$）を割り当てることができ、ユーザ２にはフィンガープリンティングワード（$\Gamma_3\Gamma_5\Gamma_2$）を割り当てることができ、全てのユーザに対し以下同様である。各々の被保護オブジェクトには、並べ替えられた形のフィンガープリンティングワードの１つが埋め込まれる。次いで、改ざんされたオブジェクトが見つかると、改ざんされたオブジェクト内のΓシンボルの各々にアルゴリズム１の原理を適用して、共謀の対象である可能性の高い色またはΓシンボルのセットが得られる。したがって、この例では、改ざんされたフィンガープリンティングワードを構成する３つのΓシンボルがある。アルゴリズム１は３つのΓシンボルの各々に適用される。この計算の結果、改ざんされたフィンガープリンティングワードの各Γシンボルに対して１セットの色またはΓシンボルが得られる。したがって、改ざんされたフィンガープリンティングワードの第１Γシンボルに対して、色（１、２、３）のセット、すなわち$\Gamma_1\Gamma_2\Gamma_3$を生成することができる。改ざんされたフィンガープリンティングワードの第２Γシンボルに対して、色（２、４）のセット、すなわち$\Gamma_2\Gamma_4$を生成することができる。改ざんされたフィンガープリンティングワードの第３Γシンボルについて、色（３、６）のセットすなわち$\Gamma_3\Gamma_6$を生成することができる。これらの結果を下の表に要約する。
【００４２】
【表６】

Γシンボル	色セット
第1Γシンボル	1, 2, 3
第2Γシンボル	2, 4
第3Γシンボル	3, 6

【００４３】
可能な色のセットの集合から、ＢＳシステムは、１つかつ唯一の色を各色セットから無作為に選択することにより、ワードまたはベクトルを作成する。この例で、ワードは、第１Γシンボルに関連付けられる色セットから色１を、第２Γシンボルに関連付けられる色セ

ットから色４を、かつ第３Γシンボルに関連付けられる色セットから色６を選択することによって作成することができる。したがって、作成されるワードは次の通り、すなわち$\Gamma_1\Gamma_4\Gamma_6$である。次いで、このワードに最も近いフィンガープリンティングワードを有するユーザが有罪とされる。ＢＳシステムおよびその証明に関するより詳細な情報は、上述した論文に見ることができる。アルゴリズム２は次の通り要約される。

【００４４】

アルゴリズム２

１．アルゴリズム１をＬ個のΓシンボルの各々に適用する。Ｌ個の構成要素の各々に対し、アルゴリズム１の出力の１つを任意に選択する。y_iをその選択された出力に設定する（y_iは［１，ｎ］の整数である）。ワードからｙ＝（y_1．．．y_L）である。

２．ｙに最も近いフィンガープリンティングワードを見つけ、対応するユーザまたはエンティティを有罪にする。

【００４５】

ＢＳシステムでは、フィンガープリンティングワードまたはシーケンスのビット長は、次式：Ｏ（c^4ｌｏｇ（Ｎ／ε）ｌｏｇ（１／ε））によって与えられる。ここで「ｃ」は共謀の規模（サイズ）であり、「Ｎ」はユーザの数であり、εは有罪判定誤り発生確率である。１ビット／秒を頑健に隠すことのできるシステムで２時間の長さのオブジェクトを保護することを希望すると想定する。Ｎ＝10^6およびε＝10^{-3}と仮定すると、防御することのできる共謀者の人数はわずかｃ＝４である。右方向の段階中に、わずか４人の共謀者に対する防御は、より多数のユーザが集まって共謀する可能性に対して防御するには充分ではない。

【００４６】

発明の方法およびシステムの概要

本発明の方法およびシステムでは、ＢＳシステムの態様をスペクトル拡散技術の使用に関連して活用する。スペクトル拡散シーケンスは、個々のフィンガープリンティングワードの個々のブロックに関連付けられる。スペクトル拡散シーケンスは、保護されるオブジェクトに埋め込まれる、「チップ」と呼ばれるデータ構造を利用する。埋込みプロセスで拡散シーケンスを使用すると、各ブロックの相対重みの再定義付けのみならず作業範囲（以下で定義する）の再定義付けも可能になる。新しい重みおよび作業範囲は、従来の方法およびシステムによって提供される以上に保護の頑健さが増強される分析に関連して利用される。

【００４７】

スペクトル拡散

発明の方法およびシステムの詳細を論じる前に、スペクトル拡散技術に関し、多少の基本的背景情報を提供する。スペクトル拡散技術に関するさらなる背景について、読者はＳｉｍｏｎ、Ｏｍｕｒａ、Ｓｃｈｏｌｔｚ、およびＬｅｖｉｔｔによって著述された「Ｓｐｒｅａｄ Ｓｐｅｃｔｒｕｍ Ｃｏｍｍｕｎｉｃａｔｉｏｎ Ｈａｎｄｂｏｏｋ」改訂版（１９９４年）と題するテキストを参照されたい。

【００４８】

保護したいオブジェクトは、ベクトルｍ＝（m_1，．．．m_u）として表わすことができる。このベクトルは、映画または何らかの種類の適切な保護するのに望ましいデジタルコンテンツの画素を表わすことができる。このベクトルの成分は、大きいアルファベットのサイズで表示される。例えばm_1は、－１２８～＋１２８の間の値を取ることのできる８ビットバイトとすることができる。保護されるオブジェクトのベクトルの個々の成分と同じ単位で測定した値を有するが、個々のベクトル成分が取ることのできる値に比較して小さい値を有する、スペクトル拡散チップｘ＝（x_1，．．．x_u）が利用される。例えばチップは｛＋１，－１｝内の値を取る。すなわち、ｘの値は、それらがｍに加えられたときに、検出することが不可能ではないにしても困難になるのに充分に小さいように選択される。

【００４９】

拡散シーケンスを利用して、｛＋１，－１｝の範囲のデータシンボルを埋め込むことができる。これらの埋込みデータシンボルは、スペクトル拡散チップが取ることのできる個々の値｛＋１，－１｝とは異なり、したがって混同を回避するためにデータシンボル｛＋１，－１｝を表わすには、表記｛＋Ｄ，－Ｄ｝を利用する。データシンボル＋Ｄまたは－Ｄが埋め込まれる場合、オブジェクトのベクトルｍは適切なスペクトル拡散チップと組み合わされる。＋Ｄを埋め込むには、拡散シーケンスをそのまま加えるが、－Ｄを埋め込む場合には、それを加える前に拡散シーケンスのチップをフリップする（すなわちシーケンスの１の補数を取る）。したがって、＋Ｄを埋め込むには、新しいベクトルｂを次式：（∀ｊ）［$b_j = m_j + x_j$］を使って計算し、－Ｄを埋め込むには、新しいベクトルｂを次式：（∀ｊ）［$b_j = m_j - x_j$］を使って計算する。そのような埋め込まれたオブジェクトを検出したとき、ベクトルｂをベクトルｘに乗じて、ベクトル成分すべてに対して総和をとる。合成ベクトル成分の総和により、当業者に理解されるように、データシンボル＋Ｄまたは－Ｄのいずれかが埋め込まれたことを指示することになる。

【００５０】

埋込み

以下の考察では、４つの特定の種類のデータ構造、すなわちチップ、ブロック、Γシンボル、およびフィンガープリンティングワードを定義し、埋込み／検出プロセスで使用する。後者の３つのデータ構造は、ＢＳシステムに関連して上述した名称と同じ名称を共用するが、それらの定義はそれらを全く異なるものにし、以下で明らかになるように、ＢＳシステムからはかなり逸脱する。

【００５１】

「チップ」は最小のデータ構造であり、スペクトル拡散チップを指す。スペクトル拡散チップは$x = (x_1, \ldots x_u)$と指定され、｛＋１，－１｝の値を有する。スペクトル拡散技術に関して上記で考察した通り、スペクトル拡散チップの使用を介して埋め込まれるデータシンボルは｛＋Ｄ，－Ｄ｝である。「ブロック」はｄ個のチップから成り、ここでｄは誤り率を制御するパラメータを表わす。ブロックは$C_1 \ldots C_k$と指定され、ここで個々のブロックｉは$C_i = (c_{i1} \ldots c_{id})$と定義され、$c_{i1} \ldots c_{id}$は個々のスペクトル拡散チップを構成する。ブロック$C_i$の１の補数は$C'_i$と表わされる。「Γシンボル」は複数のブロックを含む。記載する実施形態では、Γシンボルは２ｃ－１個のブロックから成り、ここでｃは防御したい共謀者の人数を表わす。データ構造の最後はフィンガープリンティングワードであり、これはＬ個のΓシンボルから成る。ここでＬは、関連ユーザ母集団中のユーザ全員が一意のフィンガープリンティングワードを受け取ることを確実にするように選択される特定の数を表わす。

【００５２】

各ユーザは最初に一意のフィンガープリンティングワードを割り当てられる。記載する実施形態では、フィンガープリンティングワードは、ＢＳシステムのように個々のビットではなく、スペクトル拡散を組み込む。具体的には、記載する実施形態では、ＢＳシステムのΓコードの各ブロックB_iが適切な拡散シーケンスに置換される。この例では、ＢＳシステムでI^dと想定されたブロックがC_iと置換され、0^dと想定されたブロックが１の補数C'_iと置換される。この実施形態による例示的Γコードを図３に示す。ひとたびユーザに彼らのフィンガープリンティングワードが割り当てられると、Γコードの列が、上述の通り、（チップレベルで）並べ替えられる。今、オブジェクトは、並べ替えられたΓコードによって定義されるフィンガープリンティングワードを押捺することができる。

【００５３】

図４は、記載する実施形態による埋込み方法のステップを示す流れ図である。ステップ１００は、図３に例示を示す適切なΓコードを作成または定義する。ステップ１０２は、埋込み器およびフィンガープリントを最終的に複合する復号器のみに知らされる方法でΓコードの列を並べ替える。列の並べ替えは、ユーザ全員のチップを無作為に組み替える（全てのユーザに対し同じく並べ替える）ことによって行うことができる。並べ替えはユーザ全員に対して同じである。適切な並べ替えの一例を上に挙げた。列の並べ替えが行われた

後、ステップ１０４は、保護したい多数の様々なオブジェクトの各々に一意のフィンガープリンティングワードを埋め込む。埋込みプロセスの一例をすぐ下に挙げる。埋込みプロセスの後、被保護オブジェクトを配布することができる。

【００５４】

保護されるオブジェクトまたは信号を表わすベクトルｍ＝（m_1，．．．m_u）を定義すると仮定する。拡散シーケンスｘ＝（x_1，．．．x_u）は埋込み拡散シーケンスとして使用される。ここで（∀ｊ）［$x_j \in \{+1, -1\}$］であり、信号は大きいアルファベットであり、そのサイズはこの考察では重要ではない。オブジェクトにデータシンボル＋Ｄ（または－Ｄ）が埋め込まれると、結果的に得られるマーク付けされた信号はｂ＝｛b_1．．．b_k｝と指定される。ここで（∀ｊ）［$b_j = m_j + (-) x_j$］である。

【００５５】

また、敵対者が、各構成要素にノイズ要素J_iを加えることによって、被保護オブジェクト信号をジャミング（ｊａｍ）しようとする場合をも想定する。ここでJ_iは拡散シーケンスと同じエネルギレベルである。すなわち$J_i \in \{+1, -1\}$であるが、それは拡散シーケンスとは相関されない。ジャミング攻撃の後、信号はａ＝（a_1．．．a_u）で表わすことができる。ここで（$\forall_j$）［$a_j = m_j + - x_j + J_i$］である。したがって、ベクトルａは、検出器によって見える被保護オブジェクトを表わす（すなわち埋込み後およびジャミング攻撃後）。

【００５６】

チップの検出

オブジェクトを受信したときの検出プロセスの第１ステップは、以前に並べ替えられた列の並べ替えを解除することである。フィンガープリンティングワードが割り当てられた後、オブジェクトが埋め込まれる前に、Γコードの列が（チップレベルで）無作為に並べ替えられることを思い出されたい。埋込み器および検出器は両方とも、無作為の並べ替えを知っている。列が並べ替えを解除された後、受信したオブジェクト内のチップが検出される。この例では、受信したオブジェクトはａ＝（a_1．．．a_u）と表わされ、チップは受信したオブジェクトを元の期待されるオブジェクトｍ＝（m_1，．．．m_u）と比較することによって検出される。各構成要素、例えば画素a_iが、期待されるフィンガープリンティングされていない構成要素、例えば画素m_iと比較される。次の表はこの比較およびその結果を記載する。我々は、検出されたチップｉを表わすのにz'_iを使用する。これは、攻撃のため、元のチップx_iとは異なるかもしれない。

【００５７】

【表７】

比較	結果
$a_i > m_i$	チップ $z'_i = +1$
$a_i < m_i$	チップ $z'_i = -1$
$a_i = m_i$	チップ $z'_i = 0$

【００５８】

個々のチップが識別されたので、注意は今や、共謀を構成しているらしいユーザの検出に移る。

【００５９】

クリッピング

記載する実施形態では、フィンガープリンティングワードの各ブロックはｄ個のチップを含む。これらのチップは上述した通り、前に検出されている。チップが検出された状態で、いわゆる「可視」ブロックと「不可視」ブロックを区別するために、フィンガープリンティングワードを構成するブロックが最初に「クリップ」される。「可視」ブロックとは、それらの相違のため、２人または３人以上のユーザまたはエンティティによって突き止

めることのできるブロックであることを思い出されたい。代替的に、「不可視」ブロックとは、それらが同一であるために、ユーザが「見る」ことができないブロックである。したがって、後述する通りブロックをクリップすることにより、「可視」ブロックと「不可視」ブロックを区別する。

【００６０】

以下の考察では、分析は、そのシンボルがΓシンボルであるアルファベットのブロック、Γシンボル、および誤り訂正コードを取り扱う。第１ステップで、相対重みを計算することのできる関数が定義される。この関数は次のように定義される。

【００６１】

ｘ∈｛１，－１｝およびｙ∈｛０，１，－１｝とし、関数を次のように定義する。
ｘがｙに等しくなく、かつｙが０でない場合、ｆ（ｙ，ｘ）＝１であり、
それ以外の場合、ｆ（ｙ，ｘ）＝０とする。

【００６２】

x_i∈｛１，－１｝で、Ｘ＝（x_1，．．．，x_d）とし、かつy_i∈｛１，－１，０｝で、Ｙ＝（y_1，．．．，y_d）とする。Ｘに対するＹの重みはｗ（Ｙ，Ｘ）であり、これはｉ＝１からｄまでのｆ（y_i，x_i）の和である。文脈から基準点Ｘが分かれば、我々はそれを省いてｗ（Ｙ）と書く。

【００６３】

このことから、元のブロックｉが値C_i'を有する場合（「軽ブロック」）、C_i'に対するその重みは０となる。これは、ジャミングの後も真である。他方、元のブロックがC_iであった場合（「重ブロック」）、最大ジャミング後のC_i'に対するその重みは平均ｄ／２と偏差０（$(d)^{1/2}$）を有する。これは、作業範囲が大まかにｄ／２であることを意味する。

【００６４】

上記の関数が定義されると、今度は、重み割当ておよびクリッピングのステップを行うことができる。記載する実施形態では、これは、各々ｄ個のチップのブロック（B_1，B_2，．．．）として配列された、検出されたチップz_iを入力として受け取ることによって行われる。重み割当ておよびクリッピングのステップの出力は各ブロックの相対重みであり、「見えない」可能性が高いブロックがそれらの作業範囲値にクリップされる。これは、数学的に次のように表わすことができる。

【００６５】

入力：各々ｄ個のチップのブロック（B_1，B_2，．．．）として配列された、検出されたチップｚ＝（z_1，z_2，．．．）
出力：各ブロックについてB_iはその相対重みw_i＝ｗ（B_i，C_i'）を出力し、見えない可能性の高いブロックをそれらの作業範囲値にクリップする。
方法：μ＝ｄ／２と定義し、δをこのすぐ下で定義するパラメータとする。
各ブロックB_iについて｛
ｗ（B_i）＞（１－δ）μの場合は、w_i＝（１－δ）μと設定し、
それ以外の場合は、w_i＝ｗ（B_i，C_i'）と設定する。
｝

【００６６】

パラメータの選択：
Ｎ人のユーザの場合に、誤り発生確率εでサイズｃの共謀を防御したいと想定して、次のように選択する。
・フィンガープリンティングワード当たりのΓシンボルの数＝Ｌ＝２ｃｌｎ（２Ｎ／ε）
・ブロックサイズ＝ｄ＝８c^2ｌｎ（８ｃＬ／ε）
・ｆ＝２ｌｎ（４c^2ｌｎ（２Ｎ／ε）／ε）
・δ＝ｆ／√（ｄ／２）
・μ＝ｄ／２

【００６７】

図５は、一例をすぐ上に挙げた、記載する実施形態による重み割当ておよびクリッピング方法のステップを記載する流れ図を示す。ステップ２００は、フィンガープリンティングワード内に存在する第１ブロックを得る。ステップ２０２は第１ブロックの重みを計算する。記載する実施形態では、任意のブロックの重みは上述の通り計算される。ステップ２０４は、ブロックが「不可視」ブロックである可能性が高いか否かを決定し、そうであるならば、ステップ２０６でブロックの重みをその作業範囲値にクリップする。ブロックが「可視」である可能性が高い場合には、その重みは上で計算した通りである（ステップ２０８）。ステップ２１０は、追加ブロックがあるか否かを決定する。ある場合、この方法はステップ２０２に戻る。

【００６８】

改ざんされたオブジェクトｘを生成したサブセットの検出

改ざんされたフィンガープリンティングワードの様々なブロックについて重みが計算され、上述の通り作業範囲が定義されると、注意は今や、改ざんされたオブジェクトｘを生成した共謀のサブセットを突き止めることに移る。そのような共謀を突き止めるために利用する方法は、幾つかの点で、上述したＢＳシステムの方法に似ている。主要な違いは、ブロックに対し新たに定義した重みの使用のみならず、新しい作業範囲の使用にもある。

【００６９】

アルゴリズム３

ｘ∈｛０，１｝^{dk}、ｋ＝２ｃ－１と仮定し、ｘを生成した結託のサブセットを見つける（Γコード内で、ブロックは０，．．．，ｋ－１の番号を付けられ、「色」は０，．．．ｋの番号を付けられる）。

【００７０】

１．w_0＞０である場合、「色０は有罪」と出力する。

２．w_{k-1}＜ｄ／２－（ｆｄ）$^{1/2}$の場合、「色ｋは有罪」と出力する。

３．全てのｓ＝２～ｋ－２である場合、次のことを行う。

ａ．Ｋ＝ｗ（ｘ｜R_s）（ここで、重み計算の基準点は（C'_{s-1}，C'_s）である）。

ｂ．w_{s-1}＜Ｋ／２－（（Ｋ／２）ｌｎ（２ｎ／ε））$^{1/2}$の場合、「色は有罪」と出力する。

【００７１】

上述した方法は、縮小サイズを有するΓコードを使用する文脈で特に有用である。ＢＳシステムでは、Γコードのサイズが防御したい共謀者の人数に照らして考慮されるときに、縮小サイズを有するΓコードが定義されたことを思い出されたい。その例では、Γコードの各々の新しい行または色がΓシンボルを定義し、ユーザ全員のフィンガープリンティングワードを形成するために複数のΓシンボルが用いられた。各々のフィンガープリンティングワードは異なり、一意である。並べ替えられた形のフィンガープリンティングワードは、保護しようとするオブジェクトに埋め込むために使用される。各々のフィンガープリンティングワードは、ＢＳシステムの第２アルゴリズムに従って並べ替えを解除して分析したときに、共謀者を構成する可能性の高いユーザが得られる。

【００７２】

ここで記載する実施形態では、縮小サイズのΓコードも定義され、複数の色または行を含む。色または行の数は、防御したい共謀者の人数ｃの関数である。すなわち、色または行の数は、この例では２ｃと定義される。各色または行はΓシンボルを定義する。しかし、ここで定義するΓシンボルは、ＢＳシステムで定義したΓシンボルとは非常に異なる。具体的には、ここで記載する、Γコードを形成するΓシンボルは各々が、ビットの集合ではなく、拡散シーケンスを含む。特に記述した例では、フィンガープリンティングワードはＬ個のΓシンボルから構成され、ここでΓシンボルは２ｃ－１個のブロックから構成される。ブロックは今度はｄ個のチップから構成される。ここで、チップはスペクトル拡散チップである。この関係を前提として、保護されるオブジェクトを表わすベクトルのサイズは２ｄｃＬである。

【００７３】

例示的な縮小サイズのΓコードをすぐ下の表に示す。

【００７４】

【表８】

色	Γシンボル
1	Γ_1
2	Γ_2
3	Γ_3
4	Γ_4
5	Γ_5
6	Γ_6

【００７５】

ここで、Γコードを定義する６つの色がある。これらの個々の色は、特定のユーザ母集団内のユーザ全員のためのフィンガープリンティングワードを形成するためにアルファベットとして使用される。Γコードが定義された後、各ユーザまたはエンティティは、これらのΓシンボルをＬ個有するフィンガープリンティングワードを割り当てられる。ここでＬは、２人のユーザまたは２つのエンティティが同一フィンガープリンティングワードを持たないように選択される数である。それはまた誤り発生確率をも制御する。Ｎ人のユーザがあり、誤り発生確率をεとすると、Ｌ＝２ｃ＊ｌｏｇ（２Ｎ／ε）が必要である。このフィンガープリンティングワードは、後で改ざんされたオブジェクトを受け取ったときに、ユーザまたはエンティティを識別するのに役立つ。フィンガープリンティングワードが割り当てられた後、列は、埋込み器および検出器の両方に知られる方法で、無作為に並べ替えられる。列の並べ替えの後、保護したい個々のオブジェクトに、関連するユーザまたはエンティティを識別するのに一意に役立つ、並べ替えられたフィンガープリンティングワードが埋め込まれる。

【００７６】

被保護オブジェクトを改ざんする一般的な方法は、異なるエンティティまたはユーザが集まって彼らの被保護オブジェクトを比較することであることを思い出されたい。「可視」ブロックおよび「不可視」ブロックの概念は上述した通りであり、異なる共謀者によって突き止めることのできる相違点を有するブロック、および相違点が無く、共謀者が見ることのできないブロックをそれぞれ指す。上述したマーク付けの前提に従って、共謀者は彼らが見ることのできるブロックだけを操作または調整するであろうと論理的に想定される。したがって、「不可視」ブロックは、共謀者によって操作または調整されない。こうして、改ざんされたオブジェクトを受け取った場合、それは、２人またはそれ以上の共謀者によって操作されたフィンガープリンティングワードを有する。それはまた、不可視ビットに無作為のジャミングが行われる場合にも当てはまる。

【００７７】

共謀者を構成する可能性が高いエンティティの検出

操作または改ざんされたフィンガープリンティングワードはＬ個のΓシンボルを含む。記載する実施形態では、改ざんされたフィンガープリンティングワード内の個々の構成Γシンボルは各々分析され、共謀の対象である可能性が高い１つまたは複数の色のセットが作成される。改ざんされたフィンガープリンティングワード内の全てのΓシンボルがこのようにして分析されると、改ざんされたフィンガープリンティングワード内の各々のΓシンボルについて共謀の対象であるかもしれない色の徴候を含む、ｍ×Ｌ（ここでｍはΓシンボルまたは色の数であり、すなわちｍ＝２ｃである）のマトリックスが定義される。次いで、各ユーザまたはエンティティのフィンガープリンティングワードはこのマトリックスと比較される。具体的には、ユーザのフィンガープリンティングワードの各Γシンボルが、改ざんされたフィンガープリンティングワードの対応するΓシンボルに対し可能性の高

い色のセットと比較される。ユーザのΓシンボルが、色のセットの１つと一致する場合、カウンタは増分される。一致が無ければ、カウンタは増分されず、そのユーザの次のΓシンボルが検査される。全てのユーザの全てのΓシンボルを検査し終わるまで、このプロセスが続く。プロセスのこの時点で、全てのユーザが彼らのカウンタに関連付けられる値を有する。最も可能性の高い共謀者は、最も高いカウンタ値を有するユーザである。

【００７８】

図６は、記載する実施形態による検出方法のステップを記載する流れ図を示す。ステップ３００は、ユーザまたはエンティティによって改ざんされたフィンガープリンティングワードを有する被保護オブジェクトを受け取る。ステップ３０２は、改ざんされたフィンガープリンティングワードの列の（チップレベルの）並べ替えを解除する。ステップ３０４は、改ざんされたフィンガープリンティングワード内の各々のΓシンボルを評価する。記載する実施形態では、各々のΓシンボルは、アルゴリズム３（上記）をΓシンボルに適用することによって評価される。アルゴリズム３の適用により、共謀の対象である可能性が高い色のマトリックスが生成される（ステップ３０６）。記載のマトリックスの生成は、ブロックの重みがこの例ではアルゴリズム３によって指定された所定の関係を満たす場合に、Γシンボルを選択することによって行われる。次いでステップ３０８で第１ユーザのフィンガープリンティングワードを得、ステップ３１０で、ユーザのフィンガープリンティングワード内の第１Γシンボルをマトリックスからの１つまたは複数の色のセットと比較することによって、ユーザのフィンガープリンティングワードを評価する。記載する実施形態では、マトリックスはＬ個の列を持ち、各々の列はフィンガープリンティングワードの異なるΓシンボルに対応する。どの１列に対しても、アルゴリズム３によって生成される１つまたは複数の色のセットがある。列における生成された色は各々、ユーザのフィンガープリンティングワード内の対応するΓシンボルと比較するために使用される。これは、下に挙げる例でさらに明らかになるであろう。ステップ３１２は、ユーザの特定のフィンガープリンティングワードのΓシンボルが、マトリックス内の対応する列の色のセット内の色の１つと一致するかどうかを決定する。一致がある場合、ステップ３１４はユーザのカウンタを増分する。一致が無い場合、ステップ３１６は、ユーザに対する追加Γシンボルがあるかどうかを決定する。ある場合には、ステップ３１８で次のΓシンボルを得て、ステップ３１０に戻る。ユーザに対する追加Γシンボルが無い場合には、ステップ３２０で、追加ユーザがいるかどうかが決定される。追加ユーザがいる場合には、この方法はステップ３０８に戻り、新しいユーザのフィンガープリンティングワードを得る。追加ユーザがいない場合には、ステップ３２２で、最高カウンタ値を有するユーザを選択し、彼を共謀者として有罪とする。

【００７９】

上述のプロセスの理解を助けるための一例として、次のΓコードを使用する次の基本的例を考慮する。

【００８０】

【表９】

色	Γシンボル
1	Γ_1
2	Γ_2
3	Γ_3
4	Γ_4
5	Γ_5
6	Γ_6

【００８１】

各フィンガープリンティングワードが、この例では５つのΓシンボルの長さである長さＬ

を有すると想定する。５つのΓシンボルの各々にアルゴリズム３を適用することにより、次のマトリックスが得られる。

【００８２】

【表１０】

マトリックス

色	関係色Γ_1	関係色Γ_2	関係色Γ_3	関係色Γ_4	関係色Γ_5
1		X	X		
2	X				
3	X		X	X	
4					X
5		X			X
6			X		X

【００８３】

ここで、最後の５つの列の各々が、改ざんされたフィンガープリンティングワード内の個々のΓシンボルに対応し、多数の「Ｘ」マークを含む。各「Ｘ」は、特定のΓシンボルに対し、共謀の対象であるかもしれない色を示す。改ざんされたフィンガープリンティングワードの各Γシンボルは、それに関連付けられる１つまたは複数の色のセットを有する。この例では、改ざんされたフィンガープリンティングワードの第１Γシンボルについて、色２および３が共謀の対象であるかもしれない。フィンガープリンティングワードで第２Γシンボルについて、色１および５が共謀の対象であり、以下同様である。このマトリックスが定義された後、各ユーザのフィンガープリンティングワードがΓシンボル毎に、マトリックス内の対応するΓシンボルの各々の関係色（ｉｍｐｌｉｃａｔｅｄ　ｃｏｌｏｒ）と比較される。この比較を、下表に要約する。

【００８４】

【表１１】

ユーザ１のフィンガープリンティングワード	1	1	4	6	5
カウンタ１	0	1	1	1	2
ユーザ２のフィンガープリンティングワード	2	5	3	3	4
カウンタ２	1	2	3	4	5

【００８５】

ここで、ユーザ１およびユーザ２と指定された２人の仮説的ユーザがいる。各ユーザは、その構成色によって数値的に表わされる一意のフィンガープリンティングワードを有する。例えば、ユーザ１のフィンガープリンティングワードは次の通り、すなわち［（色１）（色１）（色４）（色６）（色５）］である。これはまた、（$\Gamma_1\Gamma_1\Gamma_4\Gamma_6\Gamma_5$）と表わすこともできる。この例で、二人のユーザのどちらが有罪であるかを決定するために、ユーザのΓシンボルまたは色の各々が、上のマトリックス内の対応するΓシンボルの対応する有罪とされる色（ｉｎｃｒｉｍｉｎａｔｅｄ　ｃｏｌｏｒ）に照らして検査される。ユーザがΓシンボルがマトリックスにあることが分かると、そのユーザのカウンタはそのΓシンボルに対して増分される。こうして、ユーザ１については、その第１Γシンボルは色１によって定義される。マトリックスを参照すると、第１Γシンボルについて色１は有罪でないことを示される。したがって、ユーザのカウンタは増分されない。しかし、ユーザ１の第２Γシンボル（色１によって定義される）については、色１は、改ざんされたフィンガープリンティングワードの第２Γシンボルについて関係色のセットの中にある。した

がって、カウンタは１だけ増分される。同様の分析が残りのΓシンボルの各々について、および残りのユーザの各々について続けられる。全てのユーザがマトリックスに照らして検査された後、カウンタ（最右端カウンタ列）の値が最も高いユーザが共謀者として選出される。この例では、ユーザ２のフィンガープリンティングワードと、マトリックスの有罪とされる色との間の一致が多いので、ユーザ２の方がより高いカウンタ値を有する。

【００８６】

上述の方法およびシステムは防御できる共謀者の人数を、Ｂｏｎｅｈ－Ｓｈａｗシステムによって可能となる数より、大幅に増加することができる。例えば、映画が約10^{10}個の画素を持ち、画素の１０％が充分な量であるので、データをそれらに隠すことができると仮定する。これは、この映画に関連して10^{9}個のチップを利用できることを意味する。Ｎ＝10^{6}人のユーザがおり、10^{-3}の誤り率を希望すると仮定すると、防御できる共謀者の人数はｃ＝７８となる。上記のパラメータでは、７８人の共謀者しかいないところで、我々は約１０００のエンティティを告発するかもしれないことに注意されたい。したがって、告発は繰り返し罪を犯すものに対してのみ行うべきである。しかし、数字７８は、Ｂｏｎｅｈ－Ｓｈａｗの場合のｃ＝４に比較して有利である。より多くの共謀者を防御できることにより、保護の幅が増大し、かつ望ましくはフィンガープリンティングワードがいっそう改ざんしにくくなる。パラメータｄの要求値は、$d=2c^{2}*\log(8cL/\varepsilon)$である。

【００８７】

法律に準じて、本発明を、構造および方法論的特徴に関して多少独特の言語で説明した。しかし、ここで開示した手段は本発明を実施する好適な形態を構成するものであるので、本発明は記載した特定の特徴に限定されないことを理解されたい。したがって、本発明は、均等の原則に従って適切に解釈される特許請求の範囲の適切な範囲内でその形態または変形形態のいずれでも請求される。

【図面の簡単な説明】

【図１】　本発明の様々な態様に関連して利用することのできるコンピュータシステムの線図である。

【図２】　Ｂｏｎｅｈ－Ｓｈａｗシステムに関連して様々なユーザに割当て可能な複数の値を含むテーブルである。

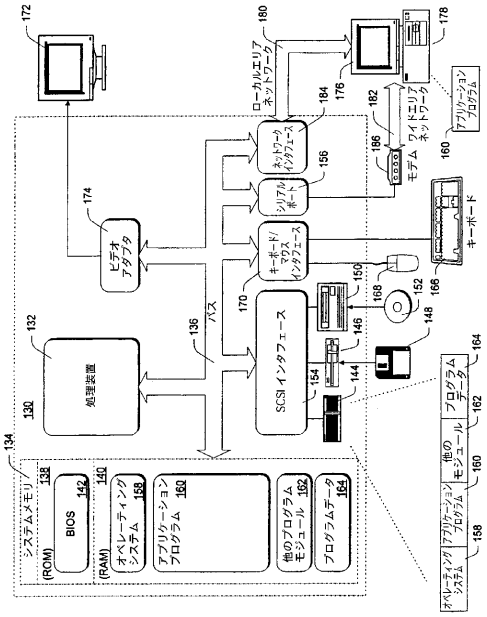
【図３】　記載する実施形態に関連して様々なユーザに割当て可能な複数の値を含むテーブルである。

【図４】　記載する実施形態による埋込み方法のステップを示す流れ図である。

【図５】　記載する実施形態による検出方法のステップを示す流れ図である。

【図６】　記載する実施形態による検出方法のステップを示す流れ図である。

【図１】



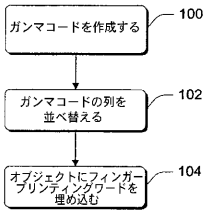
【図２】

ユーザ	ブロック０	ブロック１	ブロック２	ブロック３
1	1111	1111	1111	1111
2	0000	1111	1111	1111
3	0000	0000	1111	1111
4	0000	0000	0000	1111
5	0000	0000	0000	0000

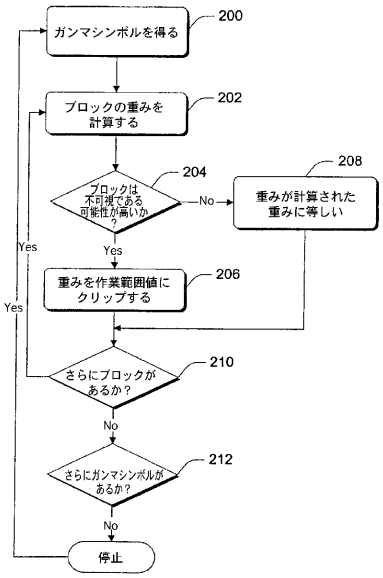
【図３】

ユーザ	ブロック０	ブロック１	ブロック２	ブロック３
1	C_0	C_1	C_2	C_3
2	C'_0	C_1	C_2	C_3
3	C'_0	C'_1	C_2	C_3
4	C'_0	C'_1	C'_2	C_3
5	C'_0	C'_1	C'_2	C'_3

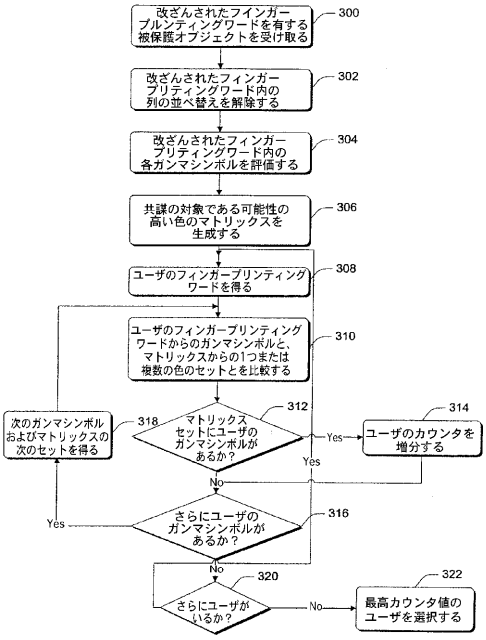
【図４】



【図５】


ガンマシンボルを得る
200
ブロックの重みを計算する
202
ブロックは不可視である可能性が高いか？
204
No
重みが計算された重みに等しい
208
Yes
Yes
重みを作業範囲値にクリップする
206
Yes
さらにブロックがあるか？
210
No
さらにガンマシンボルがあるか？
212
No
停止

【図６】


改ざんされたフィンガープルンティングワードを有する被保護オブジェクトを受け取る
300
改ざんされたフィンガープリティングワード内の列の並べ替えを解除する
302
改ざんされたフィンガープリティングワード内の各ガンマシンボルを評価する
304
共謀の対象である可能性の高い色のマトリックスを生成する
306
ユーザのフィンガープリンティングワードを得る
308
ユーザのフィンガープリンティングワードからのガンマシンボルと、マトリックスからの1つまたは複数の色のセットとを比較する
310
マトリックスセットにユーザのガンマシンボルがあるか？
312
Yes
ユーザのカウンタを増分する
314
Yes
No
次のガンマシンボルおよびマトリックスの次のセットを得る
318
Yes
さらにユーザのガンマシンボルがあるか？
316
No
さらにユーザがいるか？
320
No
最高カウンタ値のユーザを選択する
322

フロントページの続き

(74)代理人 100091063
弁理士 田中 英夫
(74)代理人 100153028
弁理士 上田 忠
(74)代理人 100120112
弁理士 中西 基晴
(74)代理人 100113974
弁理士 田中 拓人
(72)発明者 ヤコブ ヤコビ
アメリカ合衆国 ９８０４０ ワシントン州 マーサー アイランド ウェスト マーサー ウェイ ５０５０

審査官 佐田 宏史

(56)参考文献 特開平０９－１９１３９４（ＪＰ，Ａ）
欧州特許出願公開第００９５１１８３（ＥＰ，Ａ１）
特開２０００－００３１２９（ＪＰ，Ａ）
特開２０００－１６５６５４（ＪＰ，Ａ）
特開２０００－２３６４３２（ＪＰ，Ａ）
特開２０００－２７８５０４（ＪＰ，Ａ）
Ingemar J. Cox, Joe Kilian, F. Thomson Leighton, Talal Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, 米国, IEEE, １９９７年１２月３１日, Vol.6, No.12, p.1673-1687
Dan Boneh, James Shaw, "Collusion-secure fingerprinting for digital data", IEEE Transactions on Information Theory, 米国, IEEE, １９９８年 ９月３０日, Vol.44, No.5, p.1897-1905

(58)調査した分野(Int.Cl., ＤＢ名)
G06F 21/24
H04N 1/387,5/91,7/08
G09C 5/00
G06T 1/00