タイトル	ディジタルホログラフィ暗号技術のホログラムキー
著者	高井，信勝
引用	北海学園大学工学部研究報告，32：147-158
発行日	2005-02-21

ディジタルホログラフィ暗号技術のホログラムキー

高 井 信 勝*

Hologram key in digital holographic cryptography

Nobukatsu TAKAI*

Abstract

In a digital holographic cryptography, the encrypted data of a plaintext are recorded on a diffuse-type digital hologram in a randomly distributed fashion. In this report, a hologram key which locks the hologram in a way that the plaintext can never be decoded by a man not having it is investigated in some details. The condition for hologram keys is given and several kinds of hologram keys are presented. The strength of hologram keys in the cryptographic system is shown by evaluating the extent of their keyspace. As a result, the double locking system is recommended as a robust hologram key.

1．はじめに

拡散形フーリエ変換ディジタルホログラフィ[1-3]に完全復号アルゴリズム[4),5)]を用いると，あらゆるディジタルデータをディジタルホログラムとして記録（保存）し，それから１ビットの誤りもなく原データを復元できる。つまりこの技術は，画像はもとより文書データや数値データなどあらゆるディジタルデータを対象として扱うことができる。

筆者は，最近，この技術を用いて平文の文書データを暗号化するディジタルホログラフィ暗号技術を開発した[6)]。その暗号化と復号化の処理手順を図１と図２に示す。この技術は基本的に画像処理技術であって，平文の文書データは画像データと同様に扱われ，その拡散形のフーリエ変換ディジタルホログラムが平文を暗号化した記録媒体となる。図１に示す暗号化では，最初に，ホログラムからの再生像の誤差を完全に回避するために，平文データを完全復号アルゴリズムにしたがって分解し，そのディジタルホログラムを作成する。拡散形のディジタルホ

＊北海学園大学工学部電子情報工学科
Department of Electronics and Information Science, Faculty of Engineering, Hokkai-Gakuen University

ログラフィでは，任意の乱数を用いて入力データにランダム位相変調を施し，そのフーリエ変換面でディジタルホログラムが作成される。そのため，暗号化の記録媒体としてのディジタルホログラム自体の数値内容は全くランダムなものである。つまり，原データのすべての情報がディジタルホログラムの中にランダムに分散して存在する。

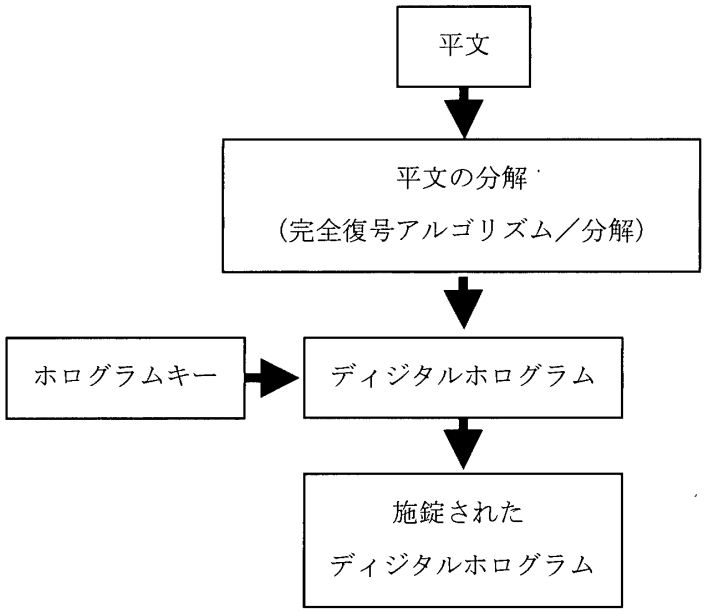

図1　ディジタルホログラフィ暗号技術における暗号化の手順。

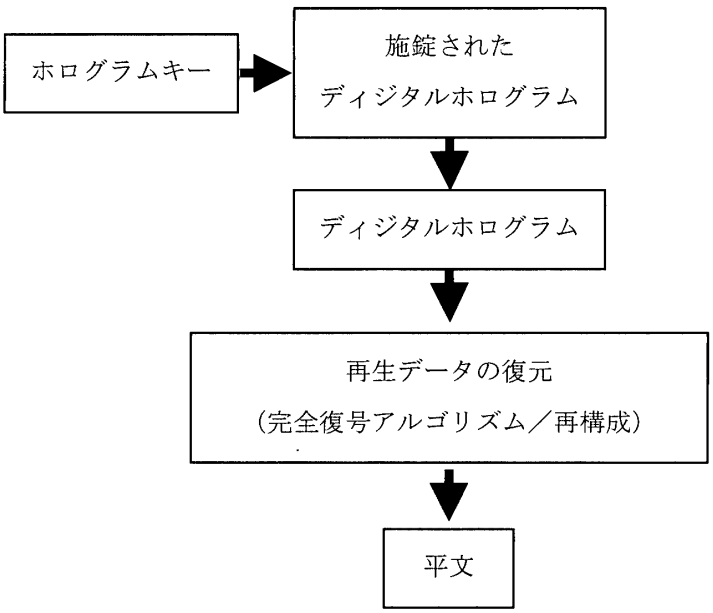

図2　ディジタルホログラフィ暗号技術における復号化の手順。

しかし，ディジタルホログラムを作成しただけでは暗号技術にはならない。ディジタルホロ

グラフィの技術と完全復号アルゴリズムは公開される技術であるので，それを知るものは誰でも復号化できる。暗号技術となるためには，暗号化と復号化のキー設定し，特定のものだけが復号できる技術でなければならない。そこで，図1に示すホログラムキーは，ディジタルホログラムから正しい再生像を得ることが不能になる処理であって，それが暗号化のために必要な要件である。

図2に示す復号化の処理では，ロッキング（施錠）されたディジタルホログラムをホログラムキーで開錠し，正規のディジタルホログラムにもどす。これによって平文を復号することができる。ただし，ホログラム再生データは完全復号アルゴリズにしたがって再構成しなければならない。このようにホログラムキーによってロッキングされたディジタルホログラムからは，たとえこの暗号技術のアルゴリズムを知っていてもホログラムキーの内容を知らなければ平文を復元することができない。

本稿では，ホログラムキーを設定する手法について報告する。暗号技術は古い歴史を持つが，近年の情報伝達はインターネットを通して行われる電子的なディジタルデータの送受信であり，暗号技術は悪意のある盗聴者から情報を守るためのコンピュータ技術として発展している[4-7]。現在，暗号技術の主流にあるDES（Data Encryption Standard）暗号やRSA暗号（R. Rivest, A.Shamir, L.Adleman暗号）は[7-10]，論理演算や数式演算による数学的な暗号アルゴリズムに基づく技術である。これらの暗号技術は，基本的に1文字1文字を他の文字や記号に置き換える「換字方式」である。一方，本稿で述べるディタルホログラフィを用いる暗号技術は光学理論と画像情報処理技術に基づくものであり，従来の暗号技術とは全く異なる発想の元で開発された技術である。したがって，ホログラムキーもまた従来にない新しい概念の暗号キーである。

2．ホログラムキーの原理

一般に，暗号技術は平文の情報を暗号化し，復号化キーをもつ特定の人だけがその情報を復号できる技術である。このとき，暗号化と復号化のアルゴリズムは公知のもので，そのアルゴリズムの実行において暗号化と復号化のキー設定がなされる。つまり，暗号技術はそれらのアルゴリズムと暗号キーの組み合わせからなっている。

ディジタルホログラフィ暗号技術では，完全復号化アルゴリズムに従って，平文を画像データと同様に扱い，それにランダム位相変調を施したのちにフーリエ変換ホログラムを作成する。そして，このホログラムから平文を復元する。この一連の手順が暗号技術としてのアルゴリズムである。したがって，これを知るものは誰でも平文を得ることができる。暗号技術であるためには，特定のものだけがディジタルホログラムから平文を復元できるキーを設定が必要

である。

暗号化／復号化のホログラムキーはホログラムに設定にできる。以下で述べるホログラムキーは，ディジタルホログラフィに用いられる完全復元アルゴリズムの有効性に基づくものである。当然のことだが，ホログラムキーが暗号化／復号化キーとなるためには，それを知らなければ平文が復元できないことが要件である。ホログラムから平文が正確に復元できるためには，完全復号アルゴリズムが有効に働くことが前提条件になる。言い換えると，ディジタルホログラムに何らかの演算を施して，完全復元アルゴリズムが破綻する状況を作ると，平文は復元できない。そして，その演算に逆演算が存在すると，ホログラム状態を元に戻すことができる。つまり，完全復号化アルゴリズムが有効になる状態にもどる。したがって，このような演算を記述できる数値パラメータが設定できると，それがホログラムキーとしてはたらく。これがホログラムキーの基本概念である。

ディジタルホログラフィ暗号技術では，画素データが8ビットからなる8ビットホログラムが暗号の記録媒体である。つまり，平文がディジタルホログラムというランダムな干渉パターンの形で暗号化される。平文の情報がディジタルホログラムから復元できると言うことは，ホログラム中にそのすべての情報がランダムに分散して記録されているからである。ところが，単に，ホログラムからいわゆる「像再生」を行うだけでは平文は正確に復元できない。正確に復元できるのは，完全復号アルゴリズムを適用し，それが有効であってはじめて達成される。この完全復元アルゴリズムは，そもそもディジタルホログラムからの再生像のすべての画素値が，確実に3ビット以下の誤差であることを前提として有効なアルゴリズムである。したがって，再生像データがそれ以上の誤差を生じるようにホログラムを細工すると，完全復号アルゴリズムは破綻する。ホログラムキーの原理はこの事実に基づいている。

平文の情報を暗号化した形で含むディジタルホログラムを$H(x,y)$とし，これに作用するホログラムキーによる演算をKで表すと，復元不能なホログラム状態$H_{Locked}(x,y)$は

$$H_{Locked}(x,y)=K\left[H(x,y)\right] \tag{1}$$

と表される（図1の施錠されたディジタルホログラム）。そして，これから平文が復元できるためには，逆演算K^{-1}が存在し，

$$H(x,y)=K^{-1}\left[H_{Locked}(x,y)\right] \tag{2}$$

が得られることである。以上のことから，ホログラムキーに課せられる要件は，つぎの二つである。

（要件1） ホログラムを元の状態に完全に戻すことができる逆演算K^{-1}が存在すること。

（要件2） $H_{Locked}(x,y)$からの再生データが3ビット以上の再生誤差を与えること。

以下では，この二つの要件を満たすホログラムキーを考察する。

3．種々のロッキング（施錠）の方法

ここでは，ホログラムキーに要求される二つの要件に関して，単一領域ホログラムキー，複数領域ホログラムキー，および，それらを繰り返して実行する多重ロッキングについて調べる。

3.1　単一領域ロッキング

ロッキングの方法：図3のように，ひとつのホログラム中にひとつの領域を設定し，その領域内のホログラムデータに演算処理を施す。これが単一領域ホログラムキーである。図4は，この領域のデータに対して考えられる演算を視覚的に示してある。この図の上段（左）を原データ（Original）とし，それを90°，180°，270°回転したRotation90，Rotation180，Rotation270を上段に，また下段には，左右および上下にデータを入れ替えたFlip left and Right, Flip up and down，さらに転置をとったTranspositionと転置を取ったのち180°回転させたTrans and Rot180の演算結果を示してある。

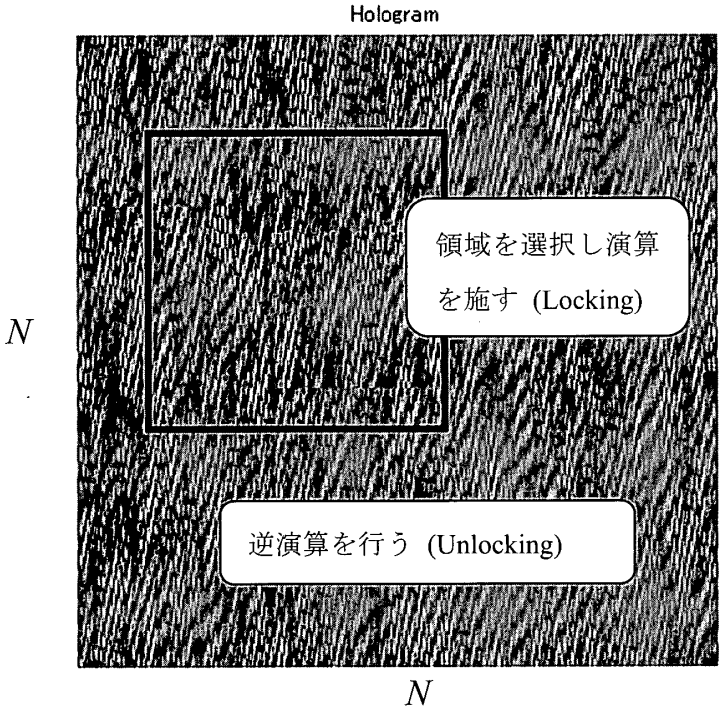

図3　単一領域ホログラムキー。この場合には，領域を指定するパラメータと演算を指定する番号がホログラムキーとなる。

この場合のホログラムキーを具体的に述べると，領域が正方領域のときには，その原点座標値と一辺の長さ，および演算を指定する選択番号がホログラムキーの内容である。領域が長方

形であれば，x軸およびy軸の両方の辺の長さが必要となる。図4は，正方領域に対する7種の演算であり，これらには逆演算が存在すること，つまり，ホログラムキーの要件（1）が満足されることは自明である。問題は，再生データが3ビット以上の再生誤差を持たなければならないホログラムキーの要件（2）である。これについては256×256の画像を用いて実験的に再生誤差を調べた。

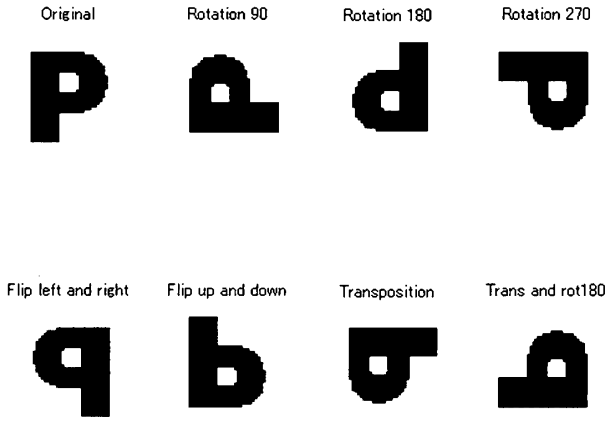

図4　単一領域ホログラムキーで用いられる演算例。

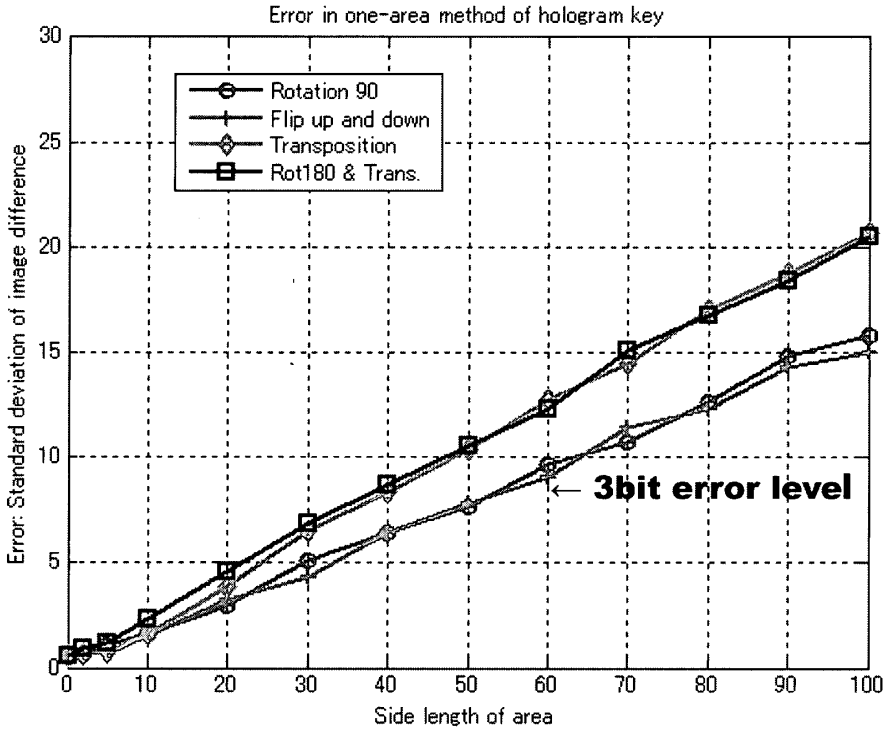

図5　単一領域ホログラムキーでロックされたホログラムからの再生像誤差（測定値）。横軸は正方領域の一辺の値（画素数），縦軸は原画像と再生画像の差の標準偏差。

図5が再生像誤差を調べた結果である。この図の横軸は正方領域の一辺の値（画素数）で，縦軸は測定された原画像と再生画像の差の標準偏差である。また，90°回転の演算が○印，上下の入れ替えの演算が＋印，転置演算が◇印，180°回転して転置をとった演算の結果を□印のマーカで示してある。この結果から，転置を用いた演算の場合（◇印と□印）が単なる回転（○）やフリップ演算（＋）の場合よりも大きな再生像誤差を与えることがわかる。これを図に示す3ビットエラーレベルで評価すると，前者では領域の一辺の長さが40程度以上で，後者では50～60程度以上で再生像誤差がそのレベルを超える。したがって，単一領域ホログラムキーでは，それよりも大きな領域を設定しなければならないので，小さい領域でホログラムキーとするときには転置を含む演算が望ましいことになる。

キー空間：単一領域ロッキングでのキー空間，すなわち考えられるキーの数はつぎのように計算される。考察したのは単純な方形の領域である。ひとつの領域は，原点座標(x,y)と辺の長さ(dx,dy)で指定できる。したがって，方形領域の位置と形を指定するには，原点のx座標値とy座標値および二辺の長さはdx, dyの4個の数値が必要である。このとき，指定する領域は既定のホログラムサイズの範囲内であり，それをはみ出すことは許されないことに注意しなければならない。そこで，ホログラムサイズを$N\times N$の場合を考え，上の4個のパラメータがいずれも最大$N/2$までの値と考えるのが現実的である。以上の条件の下で設定できる領域の数N_{1key}は，それぞれのパラメータが$N/2$個の値を独立に取り得るとすると，

$$N_{1key}=\left(\frac{N}{2}\right)^4 \qquad (3)$$

である。さらに，7種の演算を考えると，キー空間の広がりは式（3）の7倍となるが，以下の議論に合わせて領域数だけでキー空間と考えることにする。

3.2　複数領域ロッキング

ロッキングの方法：ホログラムキーの基本は，ディジタルホログラムのデータ値を欠損することなくその内部の置き換えを行うことである。このような置き換えは，複数の領域を指定して行うことができ，多様なホログラムキーを考えることができる。たとえば，同形の3つの領域を指定して，おのおのの領域のデータを循環的に入れ替えることでホログラムキーを設定できる（3領域ホログラムキー）。しかし，領域の置き換えでディジタルホログラムをロッキングする多様な方式の中で，最も重要ですべての基本となるのは2領域ホログラムキーである。

2領域ホログラムキーは，図6に示すように，同形の2つの領域A,Bのデータを入れ替える方式である。入れ替えデータを元に戻すとアンロックされる。この場合，ホログラムキーの要件1は2つの領域が重ならないかぎり成り立つ。しかし，選択した2つの領域に重なりがあると，その部分の一方のデータは消失するので，ディジタルホログラムを元の状態に戻すことが

できなくなることに注意が必要である。ホログラムキーの具体的内容は，2つの領域を指定するパラメータである。具体的には，領域A,Bの原点座標と辺の長さである。

図7に，2領域ホログラムキーでロックされたホログラムからの再生像誤差の測定値を示す。横軸は正方領域の一辺の値（画素数）で，縦軸は原画像と再生画像の差の標準偏差である。この結果は，データにゆらぎがあるとしても，領域の大きさ（辺の長さ）を大きくすると再生像誤差が単調に増加する傾向を示している。そして，要件（2）は辺の長さがおよそ30（画素）以上で満足されることがわかる。この値は，上述した単一領域ホログラムキーの場合より小さい。つまり，2領域ホログラムキーでは単一領域の場合より小さな領域でホログラムキーとしての要件が満たされる。

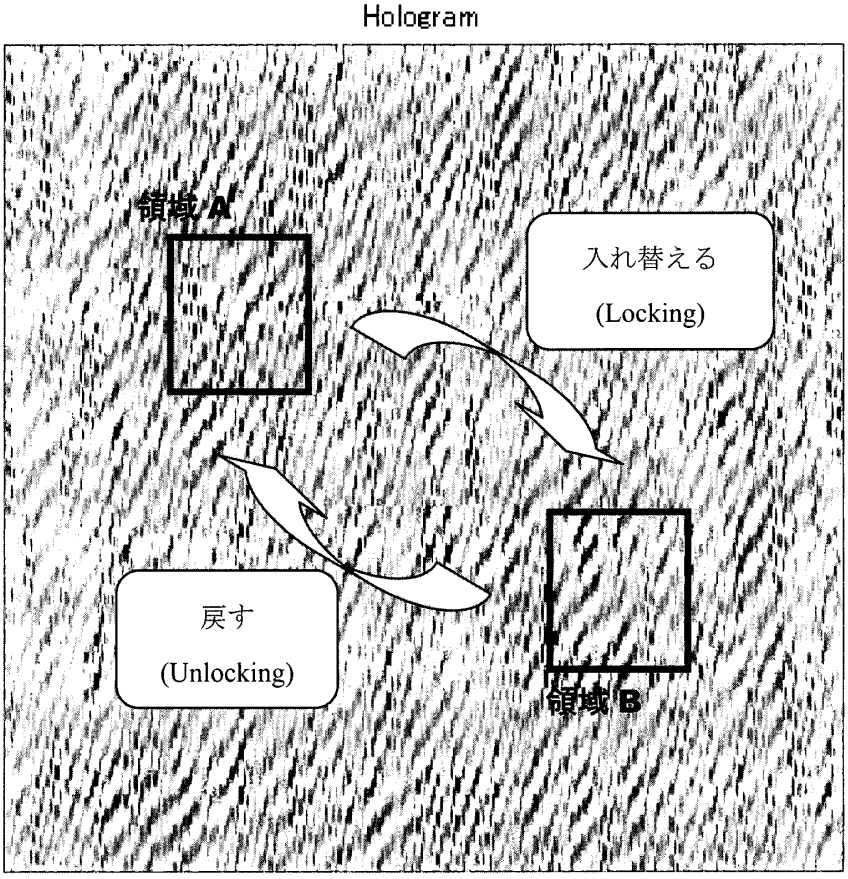

図6 2領域ホログラムキー。2つの領域を指定し，ホログラムデータを相互に入れ替えてロックする。元に戻すとアンロックされる。

キー空間：単一領域ホログラムキーの場合と同じ条件の下で2領域ホログラムキーのキー空間を計算すると次のようになる。つまり，ホログラムサイズが$N\times N$のとき，2つの領域の原点を指定する選択の数は$(N/2)^2\times(N/2)^2$であり，これに辺の長さの選択の数$(N/2)^2$を乗じることで，考えられるキーの数N_{2key}は

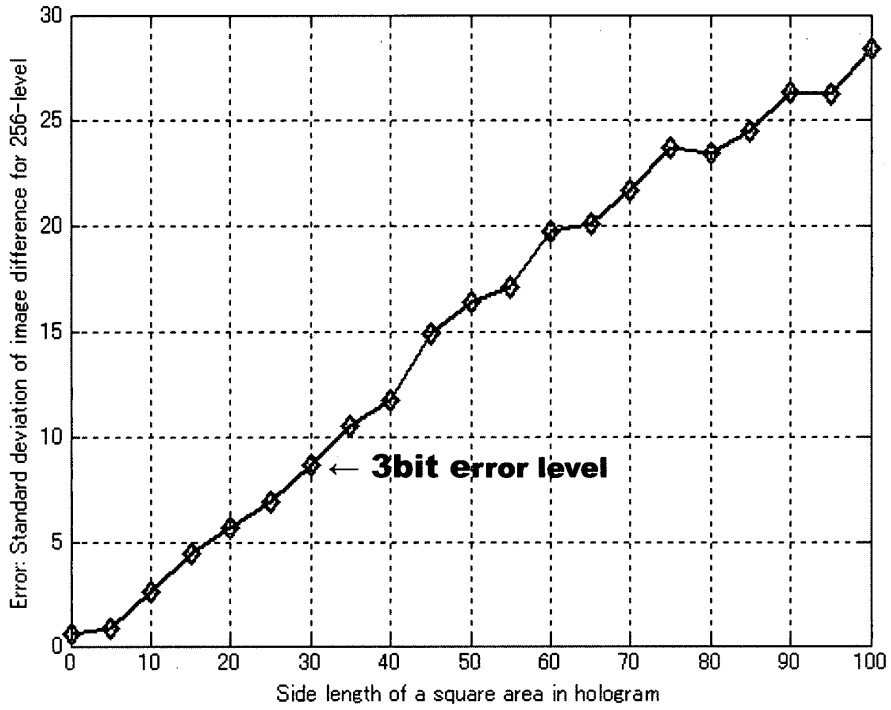

図7　2領域ホログラムキーでロックされたホログラムからの再生像誤差（測定値）。横軸は，正方領域の一辺の値（画素数）で，縦軸は，原画像と再生画像の差の標準偏差。

$$N_{2key} = \left(\frac{N}{2}\right)^6 \tag{4}$$

となる。このキー空間は，単一領域のホログラムキーのキー空間より$(N/2)^2$倍大きい。

以上の議論を推し進めると，n領域ホログラムキーでのキー空間N_{nkey}

$$N_{nkey} = \left(\frac{N}{2}\right)^{2(n+1)} \tag{5}$$

であることが知られる。しかし，ホログラムサイズは有限であるので，n個の複数領域を指定するには自ずと限界がある。

ここで，単一領域，2領域，3領域のホログラムキーに関してキー空間を表1にまとめておく。この表には，具体的にホログラムサイズが$N = 256 = 2^8$の場合のキー空間が与えられてある。また同時に，ブルート・フォース・アタック[10]（brute-force attack）いわゆる全数探索による解読時間を与えてある。この解読時間は，1攻撃あたりの処理時間を，将来の計算速度のさらなる向上と複数のコンピュータを並列に用いる攻撃を想定して10^{-9}秒として求めた。これにみられるように，単一領域ホログラムキーに対する解読時間は1秒程度にすぎず，暗号強度としては貧弱なものである。2領域ホログラムキーでは1000秒程度の解読時間であるが，通常の

コンピュータでは100倍程度の解読時間であることを考慮に入れると十分に利用できる暗号強度といえる。3領域ホログラムキーの解読時間10^8秒（約3年）は，十分な暗号強度であることを保証している。

なお，この解読時間に不安があれば，ホログラムサイズを大きくするとよい。たとえば，$N=512=2^9$とすると，2領域ホログラムキーでのキー空間は$N=2^8$の場合の2^6倍（64倍），3領域ホログラムキーでは2^8倍（256倍）になるので，キー空間はおよそ2桁大きくなる。

	単一領域ホログラムキー($n=1$)	2領域ホログラムキー($n=2$)	3領域ホログラムキー($n=3$)
キー空間（キーの数N_{nkey}）	$\left(\frac{N}{2}\right)^4$	$\left(\frac{N}{2}\right)^6$	$\left(\frac{N}{2}\right)^8$
$N=2^8$の場合のN_{nkey}	$2^{32}\approx 10^9$	$2^{42}\approx 10^{12}$	$2^{56}\approx 10^{17}$
ブルート・フォース・アタックによる解読時間	1秒	10^3秒（約17分）	10^{17}秒（約3年）

表1 複数領域ホログラムキーにおけるキー空間と解読時間（ブルート・フォース・アタックにおける1キーあたりの解読時間を10^{-9}秒とした場合）。

3.3 多重ロッキング

ロッキングの方法：多重ロッキングは，単領域ロッキングや2領域ロッキングあるいはその他の複数領域ロッキングを重ねて行う方式である。たとえば，2重ロッキングでは，図8（a）のようにA,B間の2領域ロッキングを行ったのちに，C,D間の2領域ロッキングをおこなう（同図（b））。さらに，同図（c）のように，E,F間の2領域ロッキングを行うと，3重ロッキングになる。2領域ロッキングを重ねて繰り返す多重ロッキングでは，2領域の重なりを避けると際限なく繰り返すことができる。

キー空間：2領域ホログラムキーを用いて2度ロッキングする2重ロッキングで考えられるキー数$N_{2key}^{(2)}$は，2領域ロッキングを繰り返すのであるから

$$N_{2key}^{(2)}=\left(\frac{N}{2}\right)^{12} \tag{6}$$

である。さらに，2領域ロッキング加えることで3重ロッキングすると，キー空間は

$$N_{2key}^{(3)}=\left(\frac{N}{2}\right)^{18} \tag{7}$$

となる。このように，多重ロッキングでは，キー空間の広がりは爆発的に広がる。

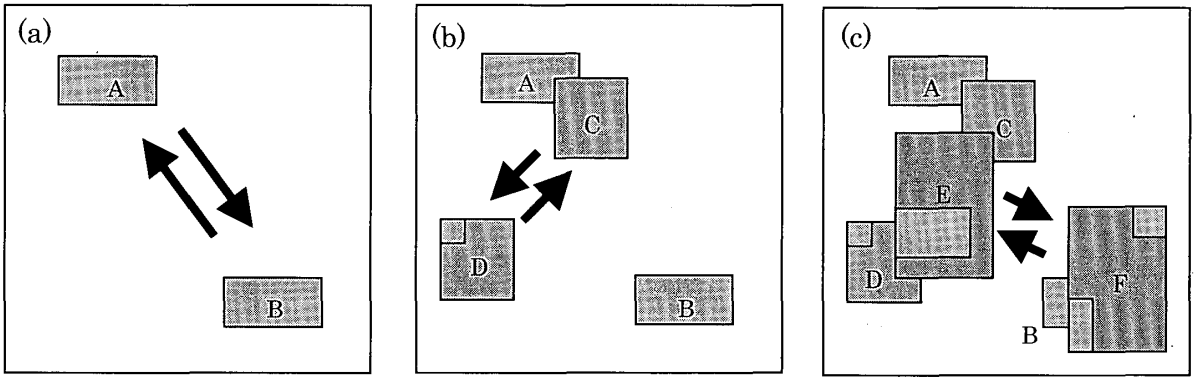

図8　多重ロッキング。(a) はA,B領域の2領域ロッキング。(b) は (a) の結果にC,D領域間の2領域ロッキングを行う2重ロッキング。(c) さらに，E,F領域の2領域ロッキングを行う3重ロッキング。

	単ロッキング ($n=1$)	2重ロッキング ($n=2$)	3重ロッキング ($n=3$)
キー空間 (キーの数$N_{2key}^{(n)}$)	$\left(\frac{N}{2}\right)^6$	$\left(\frac{N}{2}\right)^{12}$	$\left(\frac{N}{2}\right)^{16}$
$N=2^8$の場合の$N_{2key}^{(n)}$	$2^{42}\approx 10^{12}$	$2^{84}\approx 10^{25}$	$2^{126}\approx 10^{38}$
ブルート・フォース・アタックによる解読時間	10^3秒 (約17分)	10^{16}秒 (約3億年)	10^{29}秒 (約3×10^{21}年)

表2　2領域ホログラムキーにおけるキー空間と解読時間（ブルート・フォース・アタックにおける1キーあたりの解読時間を10^{-9}秒とした場合)。

表2に，ホログラムサイズが$N=256=2^8$の場合の2領域ロッキングにおけるキー空間と1攻撃あたりの処理時間を10^{-9}秒としたときのブルート・フォース・アタックによる解読時間を具体的に与えてある。ここにみられるように，2重ロッキングを用いると解読時間はおよそ3億年にもなる。この時間は現実的に解読不可能な時間といえる。

5．おわりに

本報では，最も初歩的なホログラムキーを二，三の領域キーとして紹介するとともに，そのキーを繰り返して使用する多重ロッキングについて述べた。これらの代表的な結果は，表1と表2にまとめられてある。ここでは，現実に即する具体的なキー空間とブルート・フォース・アタックによる解読時間を，1攻撃あたりの解読時間を10^{-9}秒として与えた。この結果に基づくと，2領域ホログラムキーによる2重ロッキング方式が十分な強度をもち，かつその領域構

造が簡単なことから推奨される暗号キーといえる。

二つの要件を満たすホログラムキーは，ここで述べたものの他に多種多様考えられる。たとえば，方形以外の他の形状を用いるものや格子状の領域を用いることも考えられる。また，単一領域においてデータ値を補数に置き換える方式，あるいはDES暗号のように他の領域とのXOR演算をとる方式なども考えられ，これらの研究は将来の課題として残されている。

本研究は，北海学園大学ハイテクリサーチセンター事業の研究プロジェクト「視覚・画像・音声・言語情報処理の高度化と知的計測制御技術への応用」の一環として行った。

【参考文献】

1）高井　信勝，三船　雄都，成田　貴文：デジタルホログラフィを用いる電子透かし法，北海学園大学工学部研究報告　第28号，pp.261－275（2001.2）.
2）高井　信勝：「MATLAB入門」，（工学社,2000）.
3）N.Takai and Y.Mifune：Digital watermarking by a holographic technique, Applied Optics, Vol.41, No. 5, 865－873（2002）.
4）高井　信勝：ディジタルホログラフィとその暗号化技術への応用，光技術コンタクト，第42巻，第6号,283－291（2004）.
5）高井　信勝：デジタルホログラフィを利用する暗号化データ送信方法，データ送信システム及びデータ受信システム，国際出願番号：PCT/JP2004／007412（2004）.
6）高井　信勝：拡散型ディジタルホログラフィにおける再生像の誤差評価，北海学園大学工学部研究報告，第31号，pp.87－100（2004）.
7）セアラ・フラナリー，デイヴィッド・フラナリー著，亀井よし子訳：「16歳のセアラが挑んだ世界最強の暗号」，（NHK出版，2001）.
8）サイモン・シン著，青木薫訳：「暗号解読」，（新潮社　2001）.
9）B. Schneier：Applied Cryptography, second edition（John Wiley & Sons, Inc. 2nd ed. 1996）.
10）結城　浩著：「暗号技術入門」，（ソフトバンク・パブリッシング2003）.