社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2005－ＡＶＭ－49（13）
2005／7／8

JPEG 2000 コードストリームシンタックスを利用した 画像情報の領域選択階層秘密分散法に関する検討

橋本 真幸† 南 順之‡ 松尾 賢治† 小池 淳†

†株式会社 KDDI 研究所 〒356-8502 埼玉県上福岡市大原 2-1-15
‡東京理科大学工学研究科電気工学専攻〒162-8601 東京都新宿区神楽坂 1-3
E-mail: †{masayuki, matsuo, koike}@kddilabs.jp, ‡yori-373@tsm.kddilabs.jp

あらまし 本論文では，JPEG 2000 を用いた画像情報の領域選択階層型秘密分散方式を提案する．コンテンツレベルでのセキュリティを強化するための秘密分散法に関して，完全に画像情報を再生するのに必要な数より少ない任意のシェアを集めた場合でも，部分的な画像情報あるいは画像品質をオリジナルに比べて劣化させた画像情報を提供することを可能にする．これにより，ある数以上のシェアが集まるまで情報が全く再現されない従来の完全秘密分散法を用いた分散蓄積方式に比べて，利便性が大幅に向上することが期待できる．本論文では上記実現のため，JPEG 2000 の空間的な符号化単位であるタイル構造および階層的なコードストリームシンタックスを利用する．領域選択型と階層型の 2 種類の方式を提案し，計算機シミュレーション実験により提案方式の実現可能性と有効性を示す．

キーワード JPEG 2000，秘密分散法，コンテンツレベルセキュリティ

A Study on Hierarchical-and-Region-Selective Secret Sharing Method for Images Using JPEG 2000 Code-Stream Syntax

Masayuki HASHIMOTO† Yoriyuki MINAMI‡ Kenji MATSUO† and Atsushi KOIKE†

† Visual Communication Laboratory, KDDI R&D Laboratories Inc.
2-1-15 Ohara, Kamifukuoka-Shi, Saitama, 356-8502, Japan
‡ Department of Electrical Engineering, Faculty of Engineering, Tokyo University of Science
1-3 Kagurazaka, Shinjuku-Ku, Tokyo, 162-8601, Japan
E-mail: †{masayuki, matsuo, koike}@kddilabs.jp, ‡yori-373@tsm.kddilabs.jp

Abstract This paper proposes hierarchical-and-region-selective secret sharing methods for image data in order to improve usability of the conventional secret sharing schemes using JPEG 2000 code-steam syntax. In the conventional (k, n)-threshold secret sharing scheme, secret data is reconstructed only if more shares are gathered and combined than a pre-decided number, k. Furthermore, the conventional methods are not able to reconstructed the secret data partially and hierarchically. Though large k makes a strong security feature, it creates problems with the handling of the many shares required to reconstruct the original data. Therefore, in order to improve usability, we propose two new secret sharing methods using JPEG 2000's hierarchical-and-region-selective image representation. This paper shows the feasibility and efficiency of the proposed methods by computer simulations.

Keyword JPEG 2000, Secret Searing Scheme, Contents level security

1. はじめに

ブロードバンドネットワークの整備に従いコンテンツ配信に対する注目が高まっている．コンテンツを販売することにより利益を得るビジネスを確立するためにはコンテンツに対するセキュリティは必須の技術である．秘密情報を保護し，安全に保管するための方法として秘密分散法[1]-[3]を用いた分散保管技術が注目されている．一般に良く知られている秘密分散法として(k, n)しきい値秘密分散法[1]がある．(k, n)しきい値秘密分散法は，分散関数と呼ばれる(k-1)次の多項式を使って秘密情報 S を分散符号化し，n 個の分散情報を生成する．(k, n)しきい値秘密分散法によれば n 個の分散情報のうち，任意の k 個の分散情報を集めるともとの秘密情報を復号可能であるが，(k-1)個以下の分散情報からは秘密情報を復号することは出来ない．すなわち，(k-1) 個までの分散情報が漏洩しても元の秘密

情報は復元できないため情報漏えいに対して安全であり，(n-k) 個まで分散情報が紛失しても元の情報を復元できるため，情報の紛失に対して安全である．セキュリティの度合いを上げるためにはkの値を大きくすることが望ましいが，その情報にアクセスするためには，いかなる場合でもk個以上のシェアを集めて合成する必要があり，単に画像の概要を低解像度で閲覧したい場合など，セキュリティレベルを落としても良い利用場面などでは利便性に問題が生じる可能性がある．画像情報の場合には，原画像から画質を落としたり，特定の部分にマスクがかかっていたりしても，画像の大まかな閲覧など，用途によっては問題なく利用できる場合もありえる．そこで，画像の品質を落としたり，重要な部分にのみマスクをかけるなどして，漏洩しても問題ない範囲で，低品質な画像をk個より少ないシェア数で，合成できると，より利便性が高まるものと期待できる．

そこで本論文では，合成するシェアの数により再生する画像品質を階層的に制御できる方式を提案する．上記を実現するため，JPEG 2000 (JP2) [4][5]を用いた階層符号化手法と秘密分散法を組み合わせる．JP2 においては，ウェーブレット変換やビットプレーン符号化をベースとした量子化精度の階層化を目的としたレイヤ分割により階層的に符号化が行われる．また，画像を分割して個別に符号化すること（タイル化）により，画像中の特定領域へのランダムアクセスが可能となる．

提案方式では，JP2 コードストリーム（符号列）の基本的な単位となるパケットと呼ばれるセグメントに対して，k の値を変えて分散処理を行うことにより，合成するシェアの数に応じてどのパケットが正しく再生されるかを変化させる．つまり，合成するシェア数が少ない場合は，k の値を小さく設定したパケットのみ正しく再生され，合成するシェアの数が多くなるにしたがって，k の値を大きく設定したパケットも正しく再生されるようになる．これにより，それぞれのパケットに対するkの値を適切に設定することにより，合成するシェアの数に応じて，再生画像の品質を制御することが可能となる．

以降本論文では，第 2 節で秘密分散共有法について，第 3 節で JP2 ついて概説する．第 4 節で提案方式について説明し，第 5 節で提案方式の実現可能性及び有効性を示すための実験を行う．

2. 秘密分散法

秘密分散共有法を使った情報の分散蓄積方法は図1に示すように画像情報を複数の分散情報（シェア）に分散して蓄積しておき，そのうち幾つかを合成することにより元の画像情報が得られるというものである．この方式により情報を分散して蓄積しておくことで，一部のシェアが紛失した場合でもオリジナルの画像情報の再現性が補償でき，一部のシェアが漏洩したとしてもオリジナルの情報が秘匿されるという，強固なコンテンツレベルでのセキュリティが実現される．

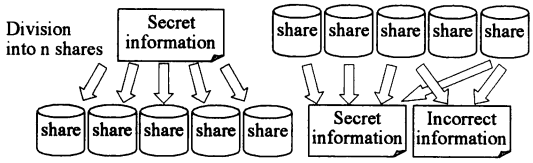


図 1　秘密分散法

一般に良く知られている Shamir の(k, n)しきい値秘密分散法では，分散関数と呼ばれる(k-1)次の多項式を用いて秘密情報を分散符号化する．分散関数の一般形は秘密情報 S，乱数項 r_i($1 \leqq i \leqq k-1$)および素数 p により次のように表現される．

$$f(x) = S + r_1 x + \cdots + r_{k-1} x^{k-1} \pmod{p} \qquad (1)$$

分散情報 W_i は上記の分散関数に任意の i(i<p)を代入し，W_i=f(i)として計算される．分散関数 f(x)は，(k-1)次の多項式であることから，k 個の分散情報を集めれば，分散関数自体を復元でき，したがって秘密情報 S の復元が可能となる．一般に，秘密分散情報 S は k 個の分散情報を表す連立方程式を解くことにより復元されるが，秘密分散法では以下の Lagrange の補間公式が用いられることが多い．

$$S = f(0) = \sum_{i=1}^{k} c_j W_i, \; which \; c_j = \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{x_j}{x_j - x_i} \qquad (2)$$

3. 階層的符号化方式 JPEG 2000

3.1. JPEG 2000 の符号化アルゴリズム

画像情報を階層的に表現する符号化手法のひとつに JP2 がある．図 2 に JP2 符号化の流れを示す．符号化対象画像は 1 つ以上のタイルと呼ばれる矩形領域に分割され，タイルごとに符号化処理される．これにより符号化データ上において特定画像領域へのランダムアクセスが容易になる．

次に，タイル化された画像はウェーブレット変換により，縦横それぞれの方向の画素値の変化の周波数成分に応じてサブバンド分解される．ウェーブレット変換は縦横両方ともが低周波数成分を持つサブバンドに対して繰り返し行われる．

サブバンドはさらに小さな矩形であるコードブロックごとにビットプレーン符号化される．図 3 にビットレーン符号化の概念図を示す．基本的には各ビット

プレーンに対して3つのパスが生成される．それぞれのパスは算術符号化される．

復号する際に読み込むビット量に応じて段階的に復号画像の画質（量子化精度）を向上させることが出来るように，符号化時に画質に同程度寄与するパスの集合をひとつのレイヤにまとめることができる．各コードブロックからのどのパスをどのレイヤに含めるかについては，各レイヤに与えられたビット量に対して，最大の画質が得られる（量子化歪が最小となる）ように，ラグランジェ未定係数法を用いたRD最適化手法を用いるのが一般的である[5]．ただし，符号化器側は規格により規定されていないために，必ずしもこれに従う必要はない．

3.2. JPEG 2000 符号列構文

符号データは，パケットと呼ばれるデータセグメント単位でまとめられる．それぞれのパケットは，必ずある特定タイルのある特定ウェーブレット分解レベルにおけるある特定レイヤの符号を含む．パケットを伝送する順序によって，再生画像の品質（解像度レベル，量子化精度，再生領域など）を柔軟に制御することが可能である．SNRスケーラブルモードの場合，あるレイヤに含まれるすべてのパケットが連続してあらわれる．より上位のレイヤのデータほどより前にあらわれる．このタイプのパケットの並びを図4(a)に示す．一方，解像度レベルスケーラブルモードの場合，ある解像度レベルに含まれるすべてのパケットが連続して現れる．より低い周波数成分を含むパケットほど前にあらわれる．この場合のパケットの並びを図4(b)に示す．

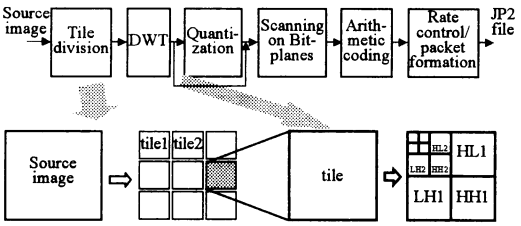


図2　JPEG 2000 符号化処理

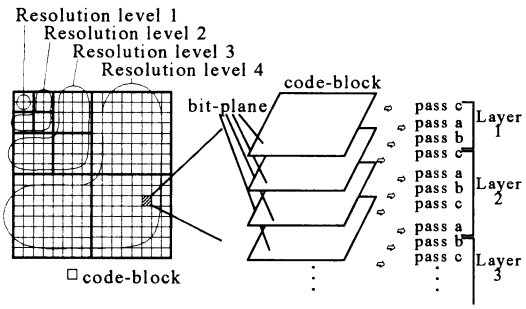


図3　符号化におけるコードブロックとパス

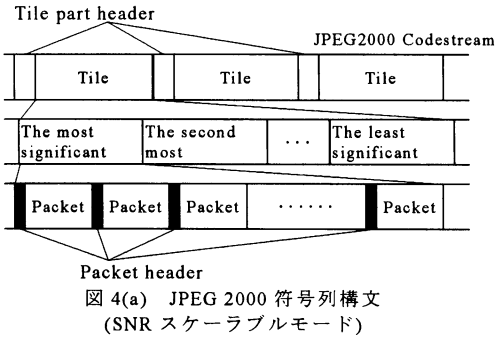


図4(a)　JPEG 2000 符号列構文
(SNR スケーラブルモード)

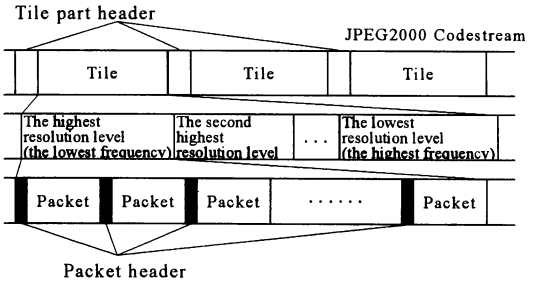


図4(b)　JPEG 2000 符号列構文
(解像度レベルスケーラブルモード)

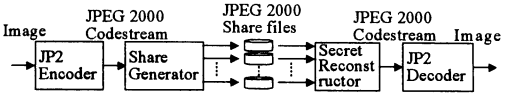


図5　提案方式のフレームワーク

4. 提案方式

4.1. 提案方式フレームワーク

画像情報の階層的秘密分散法に関して2種類の方式を提案する．方式1は領域選択型で，画像の領域に応じてセキュリティレベルを設定するものである．方式2は階層型で再生画像品質を階層的に制御する．

図5に提案方式の処理の流れを示す．まず秘密情報は符号化され通常のJP2符号列が作成される．次に，シェア作成部において，その符号列をもとに秘密分散法を用いてJP2シェア情報が作成される．ここで，領域選択機能あるいは階層的機能を実現するため，それぞれのタイルあるいはレイヤ，解像度レベルごとにkの値が決定される．

画像を再生する際にはいくつかのJP2シェア情報が合成される．まずJP2符号列が復元され，その符号列を復号して画像が再生される．提案方式においては，合成するシェア情報の数が，再生画像の再生画像領域あるいは再生画像品質に影響を与える．

4.2. 方式1:領域選択型方式

図6に提案方式1でのシェア情報生成とJP2符号列復元の様子を示す．

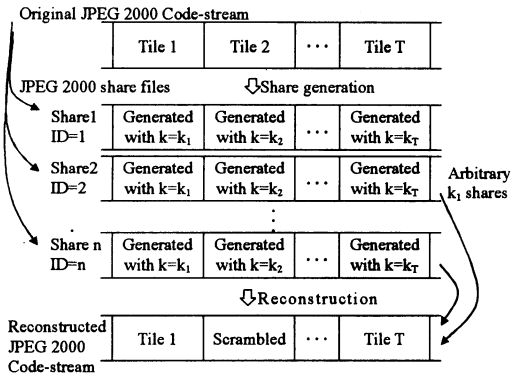


図 6　シェア情報生成と JPEG 2000 符号列の復元（領域選択型方式）

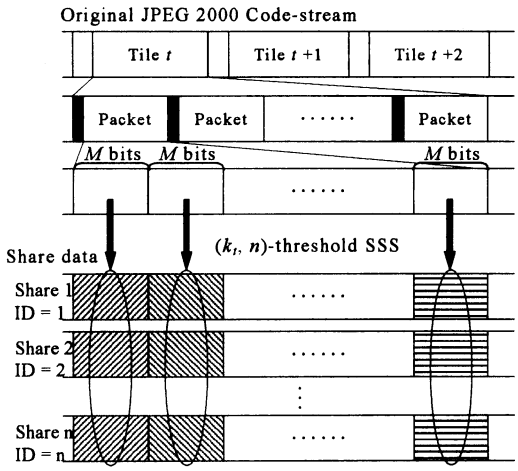


図 7　M ビットごとのシェア情報の生成

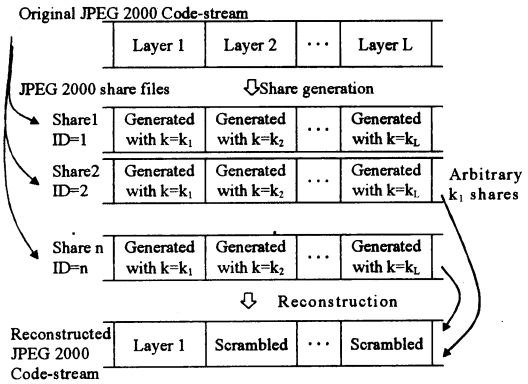


図 8　シェア情報生成と JPEG 2000 符号列の復元（階層型方式）

4.2.1. シェア情報作成処理

まず，元画像は通常の JP2 タイル符号化される．それから JP2 シェア情報が作成される．

シェア情報の作成の様子を図 7 に示す．シェア作成部では，それぞれのパケットの情報から秘密分散法を用いて n 個の分散を作成する．ここで，式(1)(2)で使われる x としてシェア ID を定義する．同図に示すように，M ビットごとに分散情報を作成し，JP2 符号列の対応するパケットデータを置き換えることで JP2 シェア情報を作成する．したがって n 個の JP2 シェア情報が作成される．それぞれのシェア ID の値はそれぞれの JP2 シェア情報のコメントタグ（自由に内容を記載できるスペース）に書き込む．後述の実験ではすべて M を 8 とした．

本方式では，それぞれのタイルに対して要求されるセキュリティレベルに応じて，あるタイルに含まれるパケットに対する k の値を 1 つ決定する．例えば，他のタイルより重要度の高い情報を含むタイルに対してはより大きな k の値を用いる．図 6 の例ではタイル 2 に対して大きな k の値を用いている．

JP2 シェア情報は，もとの JP2 符号列のパケットデータを置き換えただけのものなので，JP2 符号列構文に完全に準拠している．そのため，JP2 シェア情報を JP2 復号器で復号処理することが可能である．この場合，当然のことながら，分散処理されたタイルの部分はスクランブルされて再生される．また復号器の実装によっては，符号中にマーカコードが発生すると，復号処理に問題が発生する場合があるため，分散情報中にマーカコードが発生しないようにするのが望ましいが，ここでは他の論文（[6]など）に議論を譲る．

4.2.2. 再生処理

次に合成処理を示す．m 個の JP2 シェア情報を集めたとする．シェア情報のヘッダはコメントタグを除いては，すべて同一であるため，任意のひとつのヘッダを用いて JP2 シェア情報を解析できる．

すべてのシェア情報とコメントタグに埋め込まれた各シェア情報の ID から式(2)を用いてパケットデータを復元する．m よりも小さな k で分散処理されたタイルのパケットは正しく復元されないが，それ以外のタイルは正しく復元される．その後，通常の JP2 復号処理が行われる．前段の処理で正しく復元できていないタイルを含む場合には，その部分にノイズを含む画像が再生される．

4.3. 方式2:階層型方式

図 8 に提案方式 2 でのシェア情報生成と JP2 符号列復元の様子を示す．

4.3.1. シェア情報生成処理

まず，原画像を SNR スケーラブルモードあるいは解像度レベルスケーラブルモードで符号化し，通常の JP2 符号列を生成する．次に，方式 1 と同様に，シェア情報生成部において各パケットデータから秘密分散

法を用いて n 個の分散情報を生成する．ただし方式 2 では，どの階層要素（レイヤまたは解像度分解レベル）に含まれるパケットかによって k の値が決められる．つまり，ある階層ごとにそこに含まれるパケットに関しては特定の同一の k で分散処理を行う．もし SNR スケーラブルモードにしたければレイヤごとに k を決め，解像度レベルスケーラブルモードにしたければ解像度分解レベルごとに k を決める．

提案方式 2 では優先度の高い階層ほど小さな k の値を用いる．例えば，多くの JP2 シェア情報を合成するほど，正しく復元されるレイヤの数を増やしたい場合を考えると，シェア情報生成部においてレイヤ i に対して次のように k の値を設定して秘密分散処理を行う．

$$k_1 \le k_2 \le \cdots \le k_L \qquad (3)$$

ここで k_i はレイヤ i の秘密分散処理に用いる k の値を示し，L は JP2 符号列中のレイヤの個数を示す．

4.3.2. 再生処理

方式 2 における JP2 符号列の復元処理，画像再生処理は，基本的に方式 1 と同じである．m 個の JP2 シェア情報を合成するとする．シェア情報のヘッダはコメントタグを除いては，すべて同一であるため，任意のひとつのヘッダを用いてすべての JP2 シェア情報を解析できる．すべてのシェア情報とコメントタグに埋め込まれた各シェア情報の ID から式(2)を用いてパケットデータを復元する．もし $k_i \leqq m < k_{i+1}$ の場合には式(3)より m は k_j (j=1, 2, ⋯, i)より大きい．従って，上位のレイヤから数えて i 個のレイヤが正しく復元される．その後，通常の JP2 復号器により，復元された符号列が再生される．もし前段のパケット復元処理においていくつかのレイヤが正しく復元されていなかった場合，再生画像はノイズを含んだ画像となる．合成するシェアの数 m が増えると正しく再生されるレイヤの数が増え，再生画像のノイズ成分が減少し画質が改善する．

解像度レベルスケーラブルモードの場合は，合成するシェアの数 m が増えると正しく再生される周波数サブバンドの数が増え，再生画像のノイズ成分が減少し画質が改善する

5. 実験結果と検討

2 つの提案方式の実現可能性と有効性を検証した．

5.1. 方式1:領域選択型方式

JEPG 2000 符号化器において，図 9 に示す 20 のタイルからなる符号化を行った．そして，同図中タイル A は k = 3，タイル B は k = 2，その他のタイルに対しては k = 1 を用いて秘密分散を行った．JP2 シェア情報の数 n は 10 とした．図 10(a)にあるひとつの JP2 シェア情報から再生した画像を示す(m = 1)．図 10(b)及び図 10(c)にそれぞれ m = 2, m = 3 の場合の再生画像を示す．図 10(a)ではタイル A，B ともに画像情報が正しく再生されない．図 10(b)ではタイル A のみが正しく表示されない．図 10(c)ではすべのタイルが正しく表示されている．これはタイル A は k=3 で秘密分散処理されているため 3 つ以上のシェア情報が合成されたときのみ正しく再生され，タイル B は k = 2 で秘密分散処理されているため 2 つ以上のシェア情報が合成されたときのみ正しく再生されるためである．以上により，本提案方式では合成するシェアの数に応じて画像中の開示する領域を制御できることが確認できた．

5.2. 方式2:階層型方式

5.2.1. 解像度レベルスケーラブルモード

JEPG 2000 符号化器において 7 つの解像度レベルに分かれた通常のビットストリームを生成する．そして，周波数の低いほうから i 番目の解像度レベルの秘密分散処理に用いる k の値を k_i と定義し，シェア情報生成部において$(k_1, k_2, \cdots k_7) = (2, 3, \cdots, 8)$，n = 10 として秘密分散処理を行った．

図 11(a)にあるひとつの JP2 シェア情報から再生した画像を示す(m = 1)．図 11(b), (c), (d)および(e)にそれぞれ m = 2, 3, 4 および 8 の場合の再生画像を示す．図 11(a)からは原画像は判別できないのに対し，図 11(b)から(e)では m が大きくなるに従って再生画像中のノイズが少なくなることがわかる．これは，多くのシェア情報が合成されることにより，より多くの解像度レベルが正しく復元されるためである．本実験の場合 m = 8 以上では原画像が完全に再生される．以上の結果より，合成するシェアの数 m により再生する解像度レベルが制御でき，それにより再生画像の品質を制御できることがわかった．

5.2.2. SNR スケーラブルモード

JP2 符号化器において 4 つのレイヤを含む通常のビットストリームを生成する．この際，最上位レイヤに 0.001 bit/pixel(bpp)，2 番目の上位レイヤに 0.004 bpp，3 番目のレイヤに 0.045 bpp を割り当て，残りのビットはすべて 4 番目のレイヤに割り当てる．そして，上位 i 番目のレイヤの秘密分散処理に用いる k の値を k_i と定義し，シェア情報生成部において$(k_1, k_2, k_3, k_4) = (2, 3, 4, 5)$，n = 10 として秘密分散処理を行った．

図 12 (a)にあるひとつの JP2 シェア情報から再生した画像を示す(m = 1)．図 12(b), (c), (d)および(e)にそれぞれ m = 2, 3, 4 および 5 の場合の再生画像を示す．図 12 (a)からは原画像は判別できないのに対し，図 12(b)から(e)では m が大きくなるに従って再生画像中のノイズが少なくなることがわかる．これは，多くのシェア情報が合成されることにより，より多くのレイヤが正しく復元されるためである．本実験の場合 m =5 以上では原画像が完全に再生される．以上の結果より，

合成するシェアの数mにより再生するレイヤ数が制御でき，それにより再生画像の品質を制御できることがわかった．

6. まとめ

本論文では，秘密分散法にて画像情報を取り扱う際の利便性・機能性向上のため，JP2 を用いた画像情報の領域選択階層的秘密分散方式を提案した．提案方式1は領域選択型で，合成する JP2 シェア情報の数により再生画像中の正しく再生される領域を制御できる．提案方式2は階層型で，合成する JP2 シェア情報の数により再生画像中の正しく再生される解像度レベル数またはレイヤ数を制御でき，それにより画像品質を制御できる．シミュレーション実験により上記の実現可能性を示した．本方式により，完全に画像情報を再生するのに必要な数より少ない任意のシェア情報を集めると，周波数成分的，量子化制度的，空間領域的に画像品質を劣化させた画像情報を得ることが可能であり，ある数以上のシェアが集まるまで情報が全く再現されない従来の完全秘密分散法を用いた分散蓄積方式に比べて，利便性が大幅に向上することが期待できる．

文　献

[1] A. Shamir, "How to share a secret", In Communications of the ACM, vol.22, no.11, pp.612-613, November 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys", Proc. AFIPS 1979 National Computer Conf., vol.48, pp.313-317, September 1979.

[3] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes", J. of Cryptology, vol.4, no.2, pp.123-134, 1991.

[4] ISO/IEC 15444-1, "Information technology – JPEG2000 image coding system – Part 1: Core coding system," ISO/IEC JTC 1/SC 29/WG1, Jan.2001.

[5] D.S. Taubman, "High performance scalable image compression with EBCOT," IEEE Trans. Image Proc., vol.3 no.5, pp.1158-1170, July 2000.

[6] H. Kiya, et. al., "Partial-scrambling of images encoded using JPEG2000 without generating marker codes", IEEE International Conference on Image Processing (ICIP2003), volume 3, pp. III205-8, Sept. 2003.

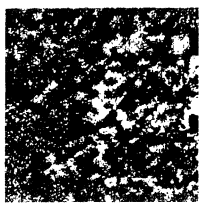
図9　タイル配置

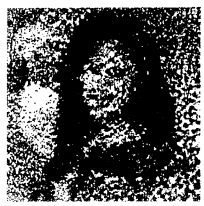

(a)Reconstructed image. m = 1. (PSNR 16.4dB)


(b)Reconstructed image. m = 2. (PSNR 21.3dB)


(c)Reconstructed image. m = 3.(Lossless)

図10　方式1の再生画像


(a)Reconstructed image. m = 1. (PSNR 7.3dB)

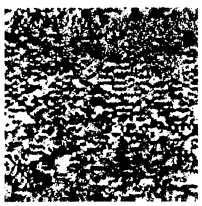

(b)Reconstructed image. m = 2. (PSNR 10.2dB)


(c) Reconstructed image m = 3. (PSNR 10.7dB)


(c)Reconstructed image. m = 4. (PSNR 11.3dB)


(d)Reconstructed image. m = 8.(Lossless)

図11　方式2の再生画像（解像度レベルスケーラブルモード）


(a)Reconstructed image. m = 1. (PSNR 6.8dB)


(b)Reconstructed image. m = 2. (PSNR 10.4dB)


(c) Reconstructed image m = 3. (PSNR 12.3dB)


(c)Reconstructed image. m = 4. (PSNR 15.6dB)


(d)Reconstructed image. m = 5.(Lossless)

図12　方式2の再生画像（SNR スケーラブルモード）