情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2009-SE-164 No.6
Vol.2009-EMB-13 No.6
Vol.2009-CSEC-45 No.6
2009/5/28

# 特定符号の発生を回避する暗号化方式及びモードの研究

池田裕樹[†1]　柿崎淑郎[†1]　岩村惠市[†1]

近年、著作権の侵害や保護が問題になっている。この問題に対してファイルフォーマットが定まった画像データを部分的に暗号化することを考える。部分的に暗号化すれば、機密を守りたいデータのみ暗号化し、それ以外は開示することで、データを復号せずともコンテンツの確認や検索が可能になる。しかし、フォーマット特有の意味を定めた系列を特定符号として設定している場合があり、部分暗号化された系列の中に特定符号と同じ符号が発生すれば、暗号化されたデータを再生器に入力した際に誤動作を引き起こすことが予想される。この問題の改善策として特定符号を回避し部分暗号化を行う手法が提案されている [1, 2]。しかし、従来の手法は非暗号化部分が一部存在する等して、安全性に問題がある。本論文では、ブロック暗号で繰り返し暗号化する部分暗号化方式を検討する。繰り返し暗号化を行うことにより、全ての暗号化対象となるデータを暗号化することが可能となり安全性が向上する。

# Researching an encryption method and each mode for outbreak evasion of the maker code

Hiroki Ikeda,[†1] Yoshio Kakizaki[†1]
and Keiichi Iwamura[†1]

The circulation of digital contents becomes popular with the development of the recent computer, the spread of network environment. While such contents can acquire easily through the Internet, the alteration of contents, infringement of copyright called an illegal copy, and protection have been a problem. When the image data to which the file format is target, technique for encrypting the part by stream cipher and block cipher is proposed as measures of the problem. However, there were the problems that there was one part or any more of the non-coding parts by these techniques. For this problem, in this paper, we suggest to encrypt it repeatedly using block cipher. By this method, Encrypting all data becomes possible.

## 1. はじめに

近年のコンピュータの高性能化、ネットワーク環境の整備・普及に伴ってディジタルコンテンツの流通が盛んになっている。ディジタルコンテンツには、画像、音声、映像などがあるが、このようなコンテンツがインターネットを介して容易に取得できるようになった反面、コンテンツの改竄や不正コピーといった著作権侵害が問題になっている。

この問題の改善策として、一般に電子透かし、ライセンス認証、データの暗号化の 3 種類の方法が存在する。データの暗号化は一般に 2 通りあり、データ全体を暗号化する方法と、データを部分的に暗号化する方法である。データ全体を暗号化すれば、情報の保護として最も安全であるが、データの一部を確認するときでも全てのデータを復号しなければならなく、制約がある。部分的に暗号化すれば、機密を守りたいデータのみ暗号化し、それ以外は開示することで、確認や検索が可能である。

本論文では、このデータの部分暗号化を考える。ここで、暗号化対象のディジタルコンテンツは、画像データとし、JPEG や MPEG のような圧縮処理が行われ、ファイルフォーマットが定まったデータを考える。画像データを暗号化する方式として、送信者と受信者が同一の暗号鍵を秘密に共有する共通鍵暗号方式を用いるとする。一般に画像データのファイルフォーマットにはそのフォーマット特有の意味を定めた系列をマーカコード（以後、特定符号）として設定している場合が多い。よって、部分的に暗号化された画像データをそのまま再生器に入力した場合、部分暗号化された系列の中に特定符号と同じ符号が発生すれば、その再生器は正常な動作をしないことが予想される。したがって、暗号化を行う場合、何らかの対策を施す必要がある。この問題に対して、文献 [1, 2] は JPEG2000 を対象として、その特定符合の発生を回避する暗号化手法が提案されている。しかし、ブロック暗号を用いる文献 [1] の手法は暗号化されている部分が非暗号化部分よりも圧倒的に少なく、暗号化部分と非暗号化部分が暗号文から容易に区別できる。ストリーム暗号を用いる文献 [2] の手法には非暗号化部分が一部存在するという問題点がある。これらの場合、攻撃者によって暗号化されたデータから元のデータを推定されてしまう可能性がある。

この問題に対して本論文では、文献 [1, 2] と同様に JPEG2000 の部分暗号化を考え、非暗号化部分をより少なく、さらには、発生させないことを目的とし、下記の要件を満たす暗

†1 東京理科大学
Tokyo University of Science

Vol.2009-SE-164 No.6
Vol.2009-EMB-13 No.6
Vol.2009-CSEC-45 No.6
2009/5/28

号化方式を提案する。

(1) 部分暗号化したデータに特定符号を含まないことが保証される。つまり、暗号化を解除せずに、部分暗号化したままのデータを再生器に入力しても再生可能である。

(2) 少なくとも暗号文攻撃と既知／選択平文攻撃対して安全性が評価されている。

(3) 非暗号化部分が文献 [1,2] に比べて少ない。

また、本論文ではブロック暗号を用いるため、主に文献 [1] の方式と比較を行うことにし、文献 [2] の概要は頁数の都合で省略する。文献 [2] の方式は、非暗号化部分が暗号文のみから判別は不可能だが、128 符号に 1 符号の割合で非暗号化部分が存在するとなっている。

## 2. JPEG2000

JPEG2000 では解像度レベルに分割した後に符号化される。したがって、高解像度部分に相当する符号列のみを部分暗号化し、低解像度部分に相当する符号列はそのままにすることにより、低解像度の画像は開示するが、高解像度画像は保護することができる。

JPEG2000 を対象とした場合、前述の特定符号とは $FF90_h$〜$FFFF_h$ の値を有するマーカ及びマーカセグメントコードを意味する。マーカとは定義情報を格納するコードである。これらは 2 バイトで表され、先頭の 1 バイトは $FF_h$ である。さらに用途に応じて $FFxx_h$ という 2 バイトデータとして表現される。一方、マーカセグメントは 1 つのマーカとそれに追随するパラメータとからなる。マーカセグメントが暗号化によってボディ部に生成されると、データの途中であるにも関わらずデータの最初や、ヘッダの終わり等と認識され誤動作することが考えられる。

特定符号には 2 つの特別な意味がある。1 つは、これらのマーカがコードストリームの区切りを意味することである。これにより、パケット及びパケットヘッダを位置づけることが可能となる。もう 1 つは、これらのマーカが圧縮データ自身の中には存在しないことである。すなわち、JPEG2000 エンコーダはこれらの特定符号をボディ部に発生させないように設計されている。よって、暗号化対象データはこのボディ部であり、その JPEG2000 データの部分暗号化において回避したいのは、$FF90_h$〜$FFFF_h$ のマーカコードの生成である。

## 3. 従 来 方 式

### 3.1 文献 [1] の概要

文献 [1] の暗号化アルゴリズムは、特定符号が $FF90_h$〜$FFFF_h$ であることに着目し、暗号化したデータに $FF_h$ が発生しないように暗号化する部分を操作することで、特定符号の発生を回避する方式である。この暗号化アルゴリズムはブロック暗号を用いる。

文献 [1] の暗号化アルゴリズムは、始めに $M$ というパラメータを定め、入力データを $M$ バイトごとに区切り、その $M$ バイトごとにランダムに定めた 1 バイトに対して、後述の暗号化アルゴリズムを実行する。また、暗号化する半バイトは次に暗号化する半バイトと合わせて 1 バイトとして、1 バイト単位に暗号化を行うブロック暗号のアルゴリズムで暗号化を行うとしている。文献 [1] の暗号化アルゴリズムは以下の通りである。

(1) $i = 1$ とする。

(2) 第 $i$ バイトを選択する。

(3) 選択されたバイトが $F0_h$ 未満ならば、その下位半バイトを暗号化する。

(4) 選択されたバイトが $F0_h$ 以上ならば、そのバイトは暗号化しない。

(5) $i$ が最終符号でなければ、$i = i + 1$ として (2) の処理から繰り返す。

3 の暗号化にはブロック暗号（Blowfish）を用い、ここで用いる暗号化アルゴリズムは安全であるとする。復号アルゴリズムは同様の逆処理を行う。

### 3.2 安 全 性

#### 3.2.1 暗号文攻撃に対する安全性

(1) 探索数に対する考察

文献 [1] の暗号化方式は下位半バイトしか暗号化しない。よって 1 バイト当たり 24 パターンで探索可能である。したがって、暗号化対象バイトが $N$ バイトの場合、最大 $24N$ が全探索数となる。$N$ が大きい場合、探索数は膨大となるが、JPEG2000 画像はパケット単位で復号できるので、パケットに含まれるバイト数が $N$ の上限となる。パケットに含まれるバイト数は選択する解像度やレイヤ数などによって異なる。よって、パケットに含まれるバイト数が少ない場合、少ない探索数で済む危険性をもつ。

(2) パラメータ $M$ に対する考察

文献 [1] の暗号化方式は、入力された全バイトを暗号化するのではなく、$M$ バイトごとにランダムに選択した 1 バイトに対して暗号化を行うことを提案している。これにより複雑度が増すとしている。1 に示した探索数は $N$ バイト中のすべての符号の暗号化部分に対して行われる探索数である。よって、$M$ に依存しないので $M$ の使用により 1 の探索数は変わらない。逆に、$M$ が用いられている場合、それを利用して以下のように 1 の探索数を減少させることが可能である。この探索は 2 段階で行われる。第 1 段階の探索では、最初 $M = N$ と仮定して、1 バイトずつ順に探索を行う。すなわち、$N$ バイト中の最初の 1 バイトに対して全パターンを試し、解読できなければそ

Vol.2009-SE-164 No.6
Vol.2009-EMB-13 No.6
Vol.2009-CSEC-45 No.6
2009/5/28

のバイトをもとに戻す。次に、次のバイトに対して全パターンを試し、解読できなければもとに戻す。この処理を最後の $N$ バイトまで行う。もし、$M = N$ であれば後述する (3) と組み合わせて、これだけの探索で解読が可能になる。よって $M = N$ の場合、$24N$ という非常に小さな探索数となる。これで解読できない場合、$M = M - 1$ として処理を継続する。最後の $N$ バイトは暗号化されているとして、残りの $M - 1$ バイトに対し 1 バイトずつ順に探索を行う。解読できなければ $M = M - 1$ として上記探索を繰り返す。すなわち、最後の $N$ または $N - 1$ バイトのどちらかが暗号化されているとして 1 バイトずつ順に探索を行うが、$N$ が暗号化された場合は前に探索済みであるので、$N - 1$ バイト目が暗号化されているとして探索を行い、意味のある画像が出力されるまで探索する。意味のある画像が探索されたとき、第 2 段階の探索に移る。文献 [1] の暗号化方式では全データを $M$ バイトごとに区切って処理を行う。よって、第 1 段階の探索によってある $M$ で意味のある画像が出力されたとき、残りのデータを $M$ バイトごとに区切って 3 と組み合わせた解読を行う。この場合、残りのデータに対しては $M$ が定まっているため 1 バイト目から $M$ バイト目までは 1 回だけ探索すればよく、$24M$ の探索数になる。この 2 段階目の探索によっても意味のある画像が出力され、かつ各 $M$ バイトごとの出力を合成して全体としても意味のある画像となるならば、その出力は正しい可能性が非常に高い。ある $M$ で解読できても、残りのデータでは解読できない場合その $M$ は間違った値であるので第 1 段階の探索の続きを行う。よって、$N$ が十分大きくても、$M$ を大きく設定している場合 1 に示した全探索数よりも非常に小さな探索数で一意に解読される危険性をもつ。

(3) 非暗号化部分を利用した解読

文献 [1] の暗号化方式は上位半バイトが常に暗号化されていない。更に、上位半バイトが $\mathrm{F}_h$ であれば下位半バイトは暗号化されない。よって、文献 [1] の暗号化方式は暗号文だけから暗号化部分と非暗号化部分が明確に区別できる。その暗号化部分を上記探索によって得られたパターンと置き換え再生を行う。文献 [1] の暗号化方式では、データの半分以上が暗号化されていないことから、意味のある画像が再生された場合、それが正しい画像でない確率は非常に少ないと思われる。よって、非暗号化部分が特定できる場合、その部分と探索パターンとの整合性から意味のある画像を絞り込むことができ、かつ非暗号化部分が多ければ多いほどその絞込みは容易になる。

#### 3.2.2 既知/選択平文攻撃に対する安全性

(1) 探索数に対する考察

文献 [1] の暗号化方式では、用いるブロック暗号は安全と仮定しているため、暗号文と平文のペアから他の暗号文を解読されることはないとしている。したがって探索数は暗号文攻撃と同じになる。

(2) パラメータ M に対する考察

$M$ が設定されている場合、暗号文と平文の比較により $M$ の値が以下のように推測できる。暗号化バイトは $M$ バイトの中からランダムに選択されるので、暗号化バイトの間隔の平均値はほぼ $M$ になると思われる。よって、既知/選択平文攻撃により明らかになった暗号化バイトからその間隔の平均値を計算し、その値を中心に探索を行えばよい。すなわち、暗号文攻撃における第 1 段階の探索を省略することができることになる。よって、既知/選択平文攻撃は暗号文攻撃より探索数を大幅に減少することができる。

(3) 非暗号化部分を利用した解読

文献 [1] の暗号化方式は暗号文だけから暗号化部分と非暗号化部分が区別できるため、既知/選択平文攻撃にしても解読の容易さは暗号文攻撃と同じである。ただし 2 から全体的には暗号文攻撃時より解読しやすくなっている。

以上から、文献 [1] の暗号化方式は非暗号化部分が多く、かつその場所が特定可能であるため、その非暗号化部分と組み合わせて意味のある画像となるパターンは限定され、解読される危険性がある。特に $M$ を大きく設定している場合、非常に少ない探索数で一意に解読される危険性が大きい。提案法は安全性を増す為に、非暗号化部分を減少させることと、暗号化部分と非暗号化部分を特定できないようにすることが目的である。

## 4. 特定符号の発生を回避する暗号化方式

### 4.1 提案方式の概要

文献 [1] の暗号化方式は、3.1 で説明したように、上位半バイトが常に暗号化されておらず、暗号化部分と非暗号化部分が、暗号文のみから明らかである。

そこで提案方式は、全てのデータを暗号化の対象とし、暗号化結果に特定符号を含むブロックが発生した場合には、そのブロックが特定符号を含まなくなるまで同じ鍵で何度も暗号化することで、特定符号の発生を回避できるようにする。例えば、3 度暗号化することによって初めて特定符号を含まない暗号化結果が出た場合に、それを最終的な暗号化結果として採用する。この時、このブロックを 1 度、2 度復号した結果には特定符号が含まれており、3 度目の復号で初めて特定符号を含まないブロックになるので、それを復号結果として

Vol.2009-SE-164 No.6
Vol.2009-EMB-13 No.6
Vol.2009-CSEC-45 No.6
2009/5/28

採用する。このとき、復号も同様に、復号結果に特定符号を含むブロックが発生した場合には、そのブロックが特定符号を含まなくなるまで同じ鍵で何度も復号することによって、元のデータに正しく復号することができる。このようにして、全てのデータを特定符号の発生を回避して暗号化することができ、正しいデータに復号することができる。

ただし、1 ブロックだけの暗号化と復号だけならば最初に述べた原理だけでよいが、複数ブロックの暗号化と復号を行う場合、ブロックの繋ぎ目において特定符号が発生した場合どのようにそれを検出するかという問題が発生する。そのために、暗号化ブロックの最終バイトが $FF_h$ であった場合にそれを記憶させ、次の暗号化ブロックの最初にそれを付け足したものを新たな暗号化ブロックとして、そのブロック内に特定符号を含んでいないか検査する。また、復号も同様に暗号化ブロックの最終バイトが $FF_h$ であった場合にそれを記憶し、次のブロックの最初にそれを付け足したものを新たなブロックとして、そのブロック内に特定符号を含んでいないかが検査される。このような状態になるときの例を下の図 1 に示す。ただし $i$ 番目のブロックを第 $i$ ブロックと呼び、それを暗号化したものを第 $i$ 暗号化ブロックと呼ぶ。図 1 に示すように、新たな第 $i$ 暗号化ブロックに特定符号が発生しているので、第 $i$ 暗号化ブロックは元のブロック内に特定符号を含んでいなくとも再度暗号化されることになる。

しかし、この手順だけでは、最終暗号化バイトが $FF_h$ で平文ブロックの最初のバイトが $90_h$〜$FF_h$ である場合、その平文ブロックをさらに復号してしまうので正しく復号できない。よって、暗号化において暗号ブロックの最終バイトが $FF_h$ である場合、予め次の平文ブロックの最初のバイトとつなげ、特定符号でないか検査してこの状況が発生しないようにする。すなわち、最終暗号化バイトが $FF_h$ で平文ブロックの最初のバイトが $90_h$〜$FF_h$ である場合、特定符号がある場合その暗号ブロックをさらに暗号化した暗号化ブロックに特定符号がなく、かつ最終バイトが $FF_h$ でなくなるまでそのブロックの暗号化を繰り返す。この処理は 4.2 の (8) によって行われる。この処理が行われれば、復号において上記状況は発生しないので、これに対応する処理は復号にはない。

以上を踏まえて、提案するブロック暗号を用いた暗号化アルゴリズムの概要は以下のようになる。ただし、文献 [1] では Blowfish を用いた 8 ビット単位の暗号化が行われていたが、ここでは安全性が評価されたブロック暗号である AES や MISTY を用いることを前提に、その暗号化単位を 1 ブロックとする。

### 4.2 暗号化アルゴリズム

4.1 で説明した提案方式の暗号化アルゴリズムを以下に示す。また、フローチャートを図 2 に示す。

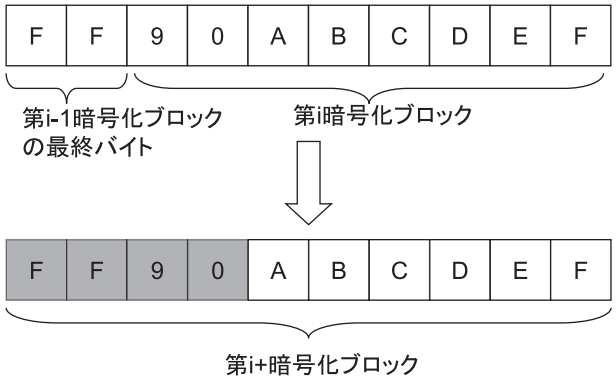


**図 1** ブロックのつなぎ目に特定符号が発生した状態

(1) $i = 1$ とする。ただし、暗号化対象は特定符号が存在しない圧縮データである。

(2) JPEG2000 ストリーム中の暗号化対象となる第 $i$ ブロックを暗号化し、第 $i$ 暗号化ブロックを出力する。

(3) 記憶させたバイトがあるか検査する。記憶させたバイトがある場合、(3y) そのバイトを第 $i$ 暗号化ブロックの先頭に連結させ、それを新たな第 $i$ 暗号化ブロックとして出力させる。

(4) 第 $i$ 暗号化ブロックに $FF90_h$〜$FFFF_h$ の特定符号が含まれていないかどうかを検査する。

(5) 記憶させたバイトがあるか検査する。記憶させたバイトがあった場合、それを取り除き、新たに第 $i$ 暗号化ブロックとして出力させる。

(6) (4) において、第 $i$ 暗号化ブロックに特定符号が含まれていた場合、(6y) 第 $i$ 暗号化ブロックを第 $i$ ブロックとし、(2) の処理から繰り返す。

(7) 第 $i$ 暗号化ブロックの最終バイトが $FF_h$ かどうかを検査する。

(8) 第 $i+1$ ブロックの最初のバイトが $90_h$〜$FF_h$ でないか検査する。第 $i+1$ ブロックの最初のバイトが $90_h$〜$FF_h$ であった場合、(2) の処理から繰り返す。そうでない場合 (8n) 第 $i$ 暗号化ブロックの最終バイトを記憶させた前のバイトに代えて、それを記憶し、第 $i$ 暗号化ブロックは第 $i$ ブロックの暗号化結果として確定される。(7) において、$FF_h$ でなかった場合、第 $i$ 暗号化ブロックは第 $i$ ブロックの暗号化結果とし

Vol.2009-SE-164 No.6
Vol.2009-EMB-13 No.6
Vol.2009-CSEC-45 No.6
2009/5/28

て確定される。

(9) 第 $i$ ブロックが暗号化対象の最後のブロックであるか検査する。最終ブロックでない場合 (9n) 第 $i$ ブロックが最終ブロックでなければ $i = i + 1$ とし (2) の処理から継続する。

### 4.3 復号アルゴリズム

提案方式の復号アルゴリズムを以下に示す。また、フローチャートを図 3 に示す。ここでは 4.2 で説明した暗号化アルゴリズムにより、複数回暗号化されたデータでも、入力される第 $i$ 番目のブロックを第 $i$ ブロックと呼ぶ。

(1) $i = 1$ とする。この JPEG2000 ストリームは予め 4.2 に示した暗号化アルゴリズムにより暗号化されたデータである。

(2) JPEG2000 ストリーム中の復号対象となる第 $i$ ブロックを復号し、第 $i$ 復号ブロックを出力する。

(3) 記憶させたバイトがあるか検査する。記憶させたバイトがあった場合、(3y) そのバイトを第 $i$ 復号ブロックの先頭に連結させ、それを新たな第 $i$ 復号ブロックとして出力させる。

(4) 第 $i$ 復号ブロックに $FF90_h$〜$FFFF_h$ の特定符号が含まれていないかどうかを検査する。

(5) 記憶させたバイトがあるか検査する。記憶させたバイトがあった場合、(5y) それを取り除き、新たに第 $i$ 復号ブロックとして出力させる。

(6) (4) において、第 $i$ 復号ブロックに特定符号が含まれていた場合には、(6y) 第 $i$ 復号ブロックを第 $i$ ブロックとし、(2) の処理から繰り返す。

(7) 第 $i$ 復号ブロックの最終バイトと第 $i + 1$ 復号ブロックの最初のバイトを連結させ特定符号か検査する。(7y) 特定符号であれば第 $i$ 復号ブロックを第 $i$ ブロックとし (2) の処理から繰り返す。

(8) 第 $i$ ブロック (入力時の暗号化ブロック) の最終バイトが $FF_h$ であるか検査する。そうであれば、(8y) 記憶させた前のバイトに代えて、それを記憶させておく。

(9) 第 $i$ 復号ブロックを第 $i$ ブロックの復号結果として確定し、第 $i$ ブロックが復号対象の最後のブロックであるか検査する。最終ブロックでない場合 (9n) 第 $i$ ブロックが最終ブロックでなければ $i = i + 1$ とし (2) の処理から繰り返す。

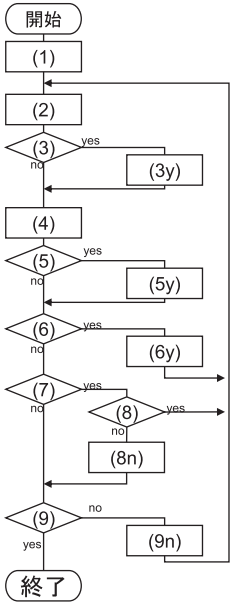


**図 2** 提案方式の暗号化アルゴリズム

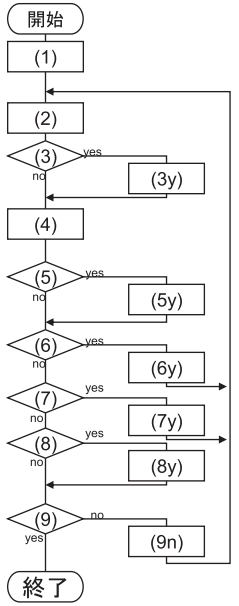


**図 3** 提案方式の復号アルゴリズム

## 5. 考　　察

### 5.1 アルゴリズムの証明

以下では暗号化アルゴリズム及び復号アルゴリズムにより次の命題が成り立つことを証明する。

**命題 1** 暗号化データは特定符号を含まない。

**命題 2** 暗号化データは正しく元のデータに復号される。

**命題 3** 暗号化したデータの全てが暗号化されている。

以下では、4.2 で定義した用語を用いることにする。

暗号化アルゴリズムは下記特徴を持つ。

**特徴 (a)** 図 2 の (2) で暗号化された結果はブロック内、もしくは前の暗号化ブロックとのつなぎ目に特定符号が含まれているとき、(2) の暗号化処理にフィードバックされる。特定符号が含まれている限り (6) でフィードバックされるため、最終暗号化結果として

Vol.2009-SE-164 No.6
Vol.2009-EMB-13 No.6
Vol.2009-CSEC-45 No.6
2009/5/28

出力されるものには特定符号が存在しない。したがって暗号化アルゴリズムは前の暗号化ブロックの最終バイトが $\mathrm{FF}_h$ であっても、暗号化ブロックおよび、前の暗号化ブロックとのつなぎ目に特定符号を含まない。

**特徴 (b)** 次のブロックとのつなぎ目にも特定符号が存在しない。

**命題 1 の証明**

(1) 第 $i$ 暗号化ブロックの最終バイトが $\mathrm{FF}_h$ ではない場合：

**特徴 (a)** より、第 $i$ 暗号化ブロックと第 $i$ 暗号化ブロックの最初のバイトと第 $i-1$ 暗号化ブロックの最終バイトには特定符号を含んでいない。いま、第 $i$ 暗号化ブロックの最終バイトは $\mathrm{FF}_h$ でないとしているので、第 $i$ 暗号化ブロックの最終バイトと第 $i+1$ 暗号化ブロックの最初のバイトとつなげたものも特定符号ではない。

(2) 第 $i$ 暗号化ブロックの最終バイトが $\mathrm{FF}_h$ である場合：

**特徴 (a)** より、第 $i$ 暗号化ブロックと第 $i$ 暗号化ブロックの最初のバイトと第 $i-1$ 暗号化ブロックの最終バイトには特定符号を含んでいない。いま、第 $i$ 暗号化ブロックの最終バイトは $\mathrm{FF}_h$ であるので、このバイトは記憶され、第 $i+1$ ブロックにおける図 2 の (3) と (4) の検査、(2) の処理により、第 $i+1$ 暗号化ブロックの最初のバイトの最終暗号化結果は $00_h$ 〜$8\mathrm{F}_h$ である。したがって第 $i$ 暗号化ブロックの最終バイトと第 $i+1$ 暗号化ブロックの最初のバイトとつなげたものも特定符号ではない。

**命題 2 の証明**

(1) 1 度暗号化した第 $i$ 暗号化ブロックに特定符号が含まれていなかった場合：

暗号化アルゴリズムにより、1 度暗号化した第 $i$ 暗号化ブロックが選択されている。このブロックを 1 度復号した第 $i$ 復号ブロックは特定符号を含まないので、復号アルゴリズムにより 1 度復号した第 $i$ 復号ブロックが選択され、正しい平文に戻すことができる。

(2) 1 度暗号化した第 $i$ 暗号化ブロックに特定符号が含まれていた場合：

暗号化アルゴリズムにより、初めて特定符号を含まなくなる $k$ 回暗号化された第 $i$ 暗号化ブロックが選択されている。このブロックを 1 回から $k-1$ 回復号した第 $i$ 復号ブロックには特定符号が含まれており、$k$ 回復号した第 $i$ 復号ブロックで初めて特定符号を含まなくなるので、復号アルゴリズムにより $k$ 回復号された第 $i$ 復号ブロックが選択され、正しい平文に戻すことができる。

(3) 第 $i-1$ 暗号化ブロックの最終バイトと、1 度暗号化した第 $i$ 暗号化ブロックの最初のバイトが特定符号でない場合：

暗号化アルゴリズムにより、1 度暗号化した第 $i$ 暗号化ブロックが選択されている。このブロックを 1 度復号した第 $i$ 復号ブロックの最初のバイトと第 $i-1$ 暗号化ブロックの最終バイトをつなげたものは、第 $i-1$ ブロックの暗号化時における図 3 のフローチャートの (6) と (7) の処理により特定符号になり得ないので、復号アルゴリズムにより 1 度復号された第 $i$ 復号ブロックが選択され、正しい平文に戻すことができる。

(4) 第 $i-1$ 暗号化ブロックの最終バイトと、1 度暗号化した第 $i$ 暗号化ブロックの最初のバイトが特定符号の場合：

暗号化アルゴリズムにより、初めて第 $i-1$ 暗号化ブロックの最終バイトと第 $i$ 暗号化ブロックの最初のバイトが特定符号でなくなる $k$ 回暗号化された第 $i$ 暗号化ブロックが選択されている。このブロックを 1 回から $k-1$ 回復号した第 $i$ 復号ブロックの最初のバイトと第 $i-1$ 暗号化ブロックの最終バイトは特定符号となる。$k$ 回復号された第 $i$ 復号ブロックの最初のバイトと第 $i-1$ 暗号化ブロックの最終バイトをつなげたものは、第 $i-1$ ブロックの暗号化時における図 2 のフローチャートの (8) の処理により特定符号になり得ないので、復号アルゴリズムにより $k$ 回復号された第 $i$ 復号ブロックが選択され、正しい平文に戻すことができる。

(5) 第 $i+1$ ブロックの最初のバイトと、1 度暗号化した第 $i$ 暗号化ブロックの最初のバイトが特定符号でない場合：

暗号化アルゴリズムにより、1 度暗号化した第 $i$ 暗号化ブロックが選択されている。このブロックを 1 度復号した第 $i$ 復号ブロックの最終バイトと第 $i+1$ ブロックの最初のバイトをつなげたものは特定符号でないので、復号アルゴリズムにより 1 度復号した第 $i$ 復号ブロックが選択され、正しい平文に戻すことができる。

(6) 第 $i+1$ ブロックの最初のバイトと、1 度暗号化した第 $i$ 暗号化ブロックの最初のバイトが特定符号の場合：

暗号化アルゴリズムにより、初めて第 $i+1$ ブロックの最初のバイトと第 $i$ 暗号化ブロックの最終バイトが特定符号でなくなる $k$ 回暗号化された第 $i$ 暗号化ブロックが選択されている。このブロックを 1 回から $k-1$ 回復号した第 $i$ 復号ブロックの最終バイトと第 $i+1$ ブロックの最初のバイトをつなげたものは特定符号となり、$k$ 回復号した第 $i$ 復号ブロックの最終バイトと第 $i+1$ ブロックの最初のバイトをつなげたものがはじめて特定符号でなくなるので、復号アルゴリズムにより $k$ 回復号された第 $i$ 復号ブロックが選択され、正しい平文に戻すことができる。

Vol.2009-SE-164 No.6
Vol.2009-EMB-13 No.6
Vol.2009-CSEC-45 No.6
2009/5/28

復号時に正しい第 $i+1$ ブロックを得られる理由について以下で説明する。まず、第 $i+1$ ブロックを復号していく過程で、最終バイトは $\mathrm{FF}_h$ にならず、第 $i+2$ ブロックの最初のバイトは $00_h$〜$8\mathrm{F}_h$ であると仮定する。

(1) 正しい第 $i+1$ ブロックの最初のバイトが $00_h$〜$8\mathrm{F}_h$ であったとする。このとき、第 $i$ 暗号化ブロックの最終バイトがどのような値でも、そのバイトと正しい第 $i+1$ ブロックの最初のバイトをつなげたものは特定符号になりえない。したがって、第 $i+1$ ブロックが複数回暗号化されていても、第 $i+1$ ブロックを複数回復号して、初めて特定符号を含まなくないブロックが正しい第 $i+1$ 復号ブロックである。

(2) 正しい第 $i+1$ ブロックの最初のバイトが $90_h$〜$\mathrm{FF}_h$ であったとする。このとき暗号化アルゴリズムにより第 $i$ 暗号化ブロックの最終バイトは $\mathrm{FF}_h$ でない。このとき、第 $i+1$ ブロックの最初のバイトがどのような値でも、第 $i$ 暗号化ブロックの最終バイトと第 $i+1$ ブロックの最初のバイトをつなげたものは特定符号になりえない。したがって、第 $i+1$ ブロックが複数回暗号化されても、第 $i+1$ ブロックを複数回復号して、初めて特定符号を含まなくないブロックが正しい第 $i+1$ 復号ブロックである。

次に第 $i+1$ ブロックを復号していく過程で、最終バイトが $\mathrm{FF}_h$ になるか、第 $i+2$ 復号ブロックの最初のバイトは $90_h$〜$\mathrm{FF}_h$ であった場合は、第 $i+2$ ブロックに関して同様に正しい第 $i+2$ ブロックを求めてから、第 $i+1$ ブロックを求めることで正しい第 $i+1$ ブロックを求めることが出来る。また、最終ブロックに関しては、次のブロックに依存しないので、最終ブロックと 1 つ前の暗号文ブロックのみから、必ず正しい復号結果が得られる、したがって、復号していく過程で最終バイトに $\mathrm{FF}_h$ が発生するブロックが連続しても、全てのデータを正しく復号することが可能である。

**命題 3 の証明**

暗号化アルゴリズムの**特徴 (b)** より、暗号化したブロックに特定符号は含まれていない。また、図 3 からわかるように、$i$ は 1 ずつ増加していき、最終ブロックに至るまで全てのブロックに対して暗号化を行っている。したがって、暗号化したデータに平文が含まれることはない。

以上より、ブロック暗号を用いた提案暗号化アルゴリズムによって暗号化したデータは**命題 1**、**命題 3** を満足し、復号アルゴリズムによって復号したデータは**命題 2** を満足する。

### 5.2 安全性および実用性の検証

**安　全　性**

提案方式は文献 [1] の暗号化方式と異なり全てのデータが暗号化されている。よって、非暗号化部分が推定されることはない。すなわち、本方式の安全性は用いるブロック暗号の安全性に依存する。

**実　用　性**

提案方式は、ブロックに特定符号が含まれなくなるまで繰り返し暗号化および復号を行うが、この繰り返しの回数により、実用性が大きく変わってくるのでステップ数を以下に示す。ここで通常のブロック暗号で 1 ブロックを 1 度暗号化することを 1 ステップと定義する。

暗号化したブロックを再び暗号化する場合は以下の 2 つの場合である。ただし、暗号化を完全なランダム化とみなし、注目する平文のバイトもランダムだと考える。

(1) 暗号化したブロックと前の暗号化したブロックの最終バイトをつなげたものに特定符号が含まれている場合

(2) 暗号化したブロックの最終バイトが $\mathrm{FF}_h$ で次のブロックの最初のバイトが $90_h$〜$\mathrm{FF}_h$ の場合

(1) の確率 は 1 ブロックに含まれるバイト数を $n$ としたとき以下の式で表せる。

$$P_1 = 1 - \left(1 - \frac{7 \times 16}{2^n}\right)^n$$

(2) の確率は以下の式で表せる。

$$P_2 = 1 - \frac{7 \times 16}{2^{16}}$$

(1) または (2) の確率で 1 ステップ増えるので、対象のデータが $N$ ブロックの場合、最終的に求めるステップ数は以下の式になる。

$$\left\{1 - P_1 + P_2 + \sum_{k=1}^{\infty}\left[\left(P_1^k + P_2^k\right)(k+1)\right]\right\} N$$

ここで、例として 16 バイト単位と 8 バイト単位のブロック暗号の場合について上式に代入して計算する。

16 バイト単位のとき $1.0344 \times N$

8 バイト単位のとき $1.0193 \times N$

以上のようになり、提案法のステップ数は通常のブロック暗号のステップ数と大差がないことがわかる。

Vol.2009-SE-164 No.6
Vol.2009-EMB-13 No.6
Vol.2009-CSEC-45 No.6
2009/5/28

## 6. ま と め

本論文では、ファイルフォーマットが定まり、かつそのフォーマット特有のマーカコードを持つデータに対して、次世代画像フォーマットである JPEG2000 を例に以下の要件を満たす暗号化方式を提案した。

(1) 部分暗号化したデータに特定符号を含まないことが保証される。つまり、暗号化を解除せずに、部分暗号化したままのデータを再生器に入力しても再生可能である。

(2) 少なくとも暗号文攻撃と既知／選択平文攻撃対して安全性が評価されている。

(3) 非暗号化部分が文献 [1,2] に比べて少ない。

その結果非暗号化部分を発生させることなく、全てのデータを暗号化することを実現した。

## 参 考 文 献

1) 貴家仁志，今泉祥子，渡邊修 :「マーカコードの発生を考慮した JPEG2000 符号化画像の情報開示法」，電子情報通信学会論文誌，Vol.J86-D-II，No.11，pp.1628–1636，2003 年 11 月.
2) 岩村惠市，林淳一 :「JPEG2000 符号化画像のマーカコード発生を回避できる暗号化方式」，電子情報通信学会論文誌，Vol.J90-A，No.11，pp.839–850，2007 年 11 月.
3) 小野定康，鈴木純司 :「JPEG2000 の技術」，オーム社，2003 年 5 月.