6Y-1

カラー画像データに適した暗号化方法の提案

諸節真喜子，古村文伸
(株)日立製作所　システム開発研究所

1．はじめに

高度情報社会への進展による情報の多様化に伴い、ディジタル画像データの利用分野が拡大し、画像情報のセキュリティ対策として暗号方式の研究の必要性が増している。本報告では、高精細なカラー画像データを対象とし、転置暗号を施したときの問題点を指摘し、カラー画像に適した暗号方式の提案を行なう。

2．転置暗号適用の問題点

ディジタル画像データの転置暗号方式としては、走査線の転置、走査線内の画素の転置が知られている[1]。圧縮効果の薄い高精細な画像においては、画像データの自己相関をなくす画素単位の転置が有効である。

しかし、この走査線内の画素の転置をカラー画像に適用した場合、赤(R)、緑(G)、青(B)に対応する各バンドごと別別に処理を行なったとすれば、転置暗号を行なっても画素値のヒストグラムは変化しないため、暗号画像に色の情報が残ってしまうという問題が起こった。

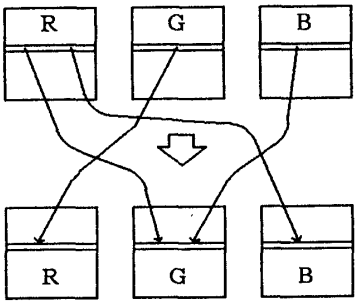
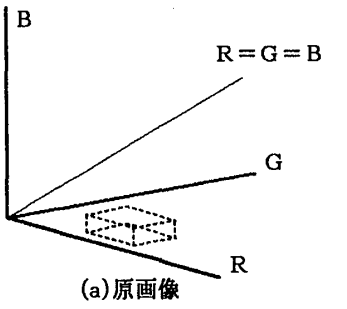


図1　カラーバンド間転置

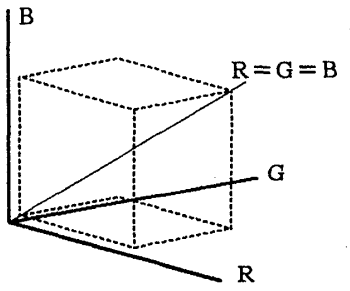
3．カラーバンド間転置暗号方式

上記問題点を解決する方法として、カラーバンド間転置暗号方式を提案する。これは、画像の各バンド間に渡って画素の入れ替えを行なうもので、RGBの各バンドに対応する3つの画像データの同位置にある走査線をまとめ、1本の走査線とみなすことで実現される。これを図1に示す。

この方法によると、転置暗号化前にはRGB空間のある色味の方向に偏っていた画素値のレベルの分布が、転置暗号化後にはRGB空間の対角線上にまたがる



(a)原画像



(b)カラーバンド間
転置方式による暗号画像

図2　画素値の分布

Proposal of an Encryption Algorithm for Color Image Data
Makiko Morofusi, Fuminobu Komura
Systems Development Laboratory, Hitachi, Ltd.

ように広がる(図２)ため、見掛け上色味が失せ無彩色のようになり、色の情報が秘匿される。

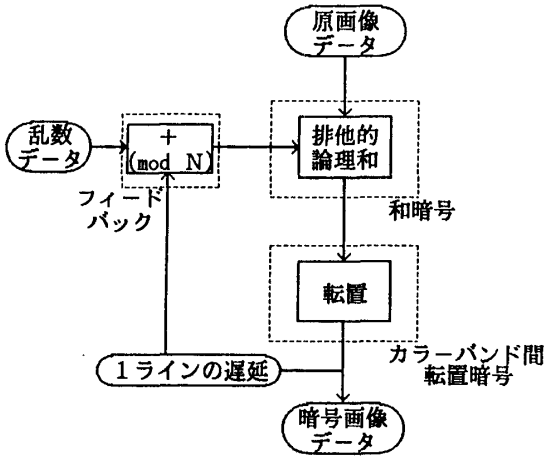
４．カラーバンド間転置を利用した暗号方式の提案

カラーバンド間転置によって色の情報は秘匿可能になったが、暗号画像データにはまだ濃淡の情報が完全に秘匿されずに残ってしまっている。このため、一様な背景部分を含む画像では、「地」の部分と「図」の部分が判ってしまうこともある。従って、より安全性を必要とする場合、雑音加算(和暗号)等を組み合わせた複合暗号方式にし、暗号強度を高めるべきである。

しかし、和暗号を組み合わせただけでは、同一鍵を用いた２枚の暗号画像の差をとることによって加算されていた雑音が相殺されてしまい、暗号強度は高くならない。そこで、和暗号とカラーバンド間転置暗号の複合方式に暗号画像データをフィードバックさせる方式を提案する。

図３は、本提案方式の暗号化処理の概要を示したものである。フィードバック処理は、ＲＧＢ３つのバンドの同位置にある走査線をまとめた１ラインを単位として行なう。ここで遅延データは、和暗号の排他的論理和と異なる、階調数の剰余系(mod Ｎ)による算術和を用いて乱数データに加算することが重要である。和暗号と異なる演算を用いることによって暗号強度が増すからである。また、遅延データを乱数データに加算することによって、暗号・復号アルゴリズムが対称的になる。

本提案方式は慣用暗号系の１つであり、鍵は乱数データの生成及び転置に用いる。



Ｎ：階調数

図３　カラー画像向き暗号提案方式
(カラーバンド間転置を利用した複合方式)

５．おわりに

転置暗号をカラー画像に適用したときに色の情報が残るという問題を、カラーバンド間転置によって解決し、本転置方式を含むカラー画像向き暗号方式を提案した。

本提案方式は、単純な処理の組み合わせによりなるため高速に処理ができ、画素値のヒストグラム情報や相関からの解読が不可能な高信頼性を持つものである。このため、特に大容量な高精細カラー画像に適した暗号化方法である。

【謝辞】

本研究は、通商産業省工業技術院大型プロジェクト「電子計算機相互運用データベースシステムの研究開発」の一環としてＩＮＴＡＰ((財)情報処理相互運用技術協会)がＮＥＤＯから委託を受けて、実施したものである。

【参考文献】

１）富永他：”機密保護を可能とするファクシミリ通信方式”，信学論Ｂ，82年11月