文書画像情報の通信セキュリティに関する研究

小松　尚久
早稲田大学　理工学部
電子通信学科　助教授

1．はじめに

ファクシミリに代表される文書画像通信は、端末の小型化と低廉化等により急速な勢いでパーソナル化が進んでいる。これに伴い、簡単な手順で個人のプライバシーを保護するセキュリティ対策の必要性がますます高くなると考えられる。また、画像データベース検索等ソフトコピー通信を念頭に置いた画像通信サービスも検討されており、こうしたアプリケーションでは正当な受信者のみに情報を提供する対策が必要となる。そこで本研究では、このように今後ますます多様化すると考えられる文書画像通信への適用を考慮したセキュリティ対策について考察を進めた。

2．ＳＦＣを用いた文書画像のスクランブル手法

(1)　文書画像の機密通信システム

文書画像通信の代表例であるファクシミリを例にとり、セキュリティ機能を有する通信システムを図１に示すとおり分類する[1]。ここで図１(a)は、本研究で対象としているシステム構成であり、暗号化された文書が符号化される構成になっている。本構成は、例えばＰＣとファクシミリ通信用ボードを利用することにより、特別なハードウェアを必要とせずに end-to-endの機密通信システムが実現できる点に特徴がある。ただし、暗号化等の手段については、画素間の相関が失われて冗長度抑圧符号化の効果を損なわないように決定する必要があり、この点で制約が加わる。また、図１(b)はネットワーク側に設置された通信アダプタで暗号化／復号を行なう構成であり、図１(c)は冗長度抑圧符号化された出力を暗号化して伝送する構成である。

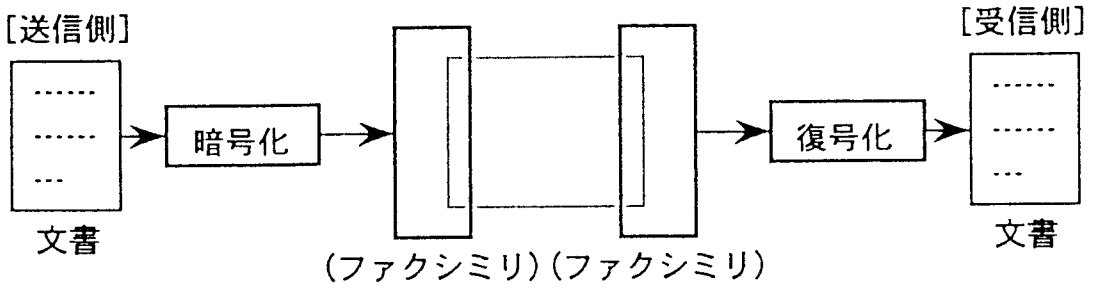
(2)　改良形ＳＦＣを用いたスクランブルアルゴリズム

図１(a)の構成で画素間の相関を失うことなく機密保護対策を講じるためには、ＤＥＳ，ＲＳＡ等の暗号アルゴリズムの使用は適していない。一方、スクランブル走査は上記の条件を満足する手段の一つとして挙げられる。さらに、走査の条件として、走査方向に規則性がなく、かつ隣接する画素が走査対象となることが望ましい。これらの条件を満たすアルゴリズムとして、Hilbert走査で代表されるＳＦＣ(Space Filling Curve) に着目した。しかしながら、ＳＦＣをそのままスクランブルアルゴリズムとして使用すると、十分なスクランブル効果が得られず安全性の面で問題が生じるため、基本走査パターンの種類を増加することを特徴とした、改良形ＳＦＣを（以下ＩＳＦＣ（Improved SFC））を提案した[2]-[4]。

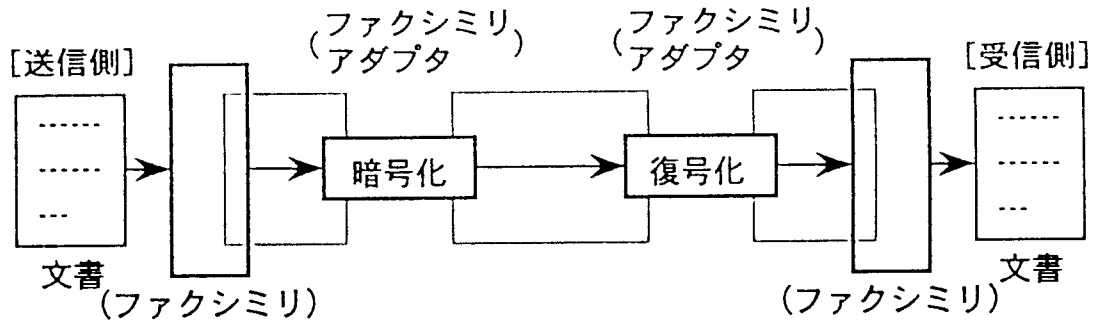
２次元空間における Hilbert走査は４種類のパターンで構成される。一方、ＩＳＦＣでは画素間を斜め方向に走査することを許容して、合計24種類の走査パターンを用いている。その結果、スクランブルを行なう鍵の候補は、

$$K_P^I = 2^{P(4-1)/3} \qquad (1)$$

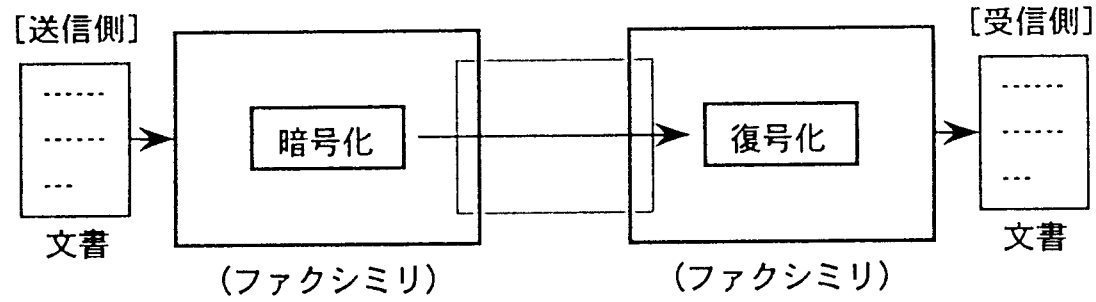
通り存在する。図2にＩＳＦＣ走査によるスクランブルパスの一例を示す。また、図3にはＩＳＦＣでスクランブル走査を行った後、デスクランブル時に異なるパスを適用した結果である。



(a) システム構成Ａ



(b) システム構成Ｂ



(c) システム構成Ｃ

図1　機密ファクシミリ通信システム

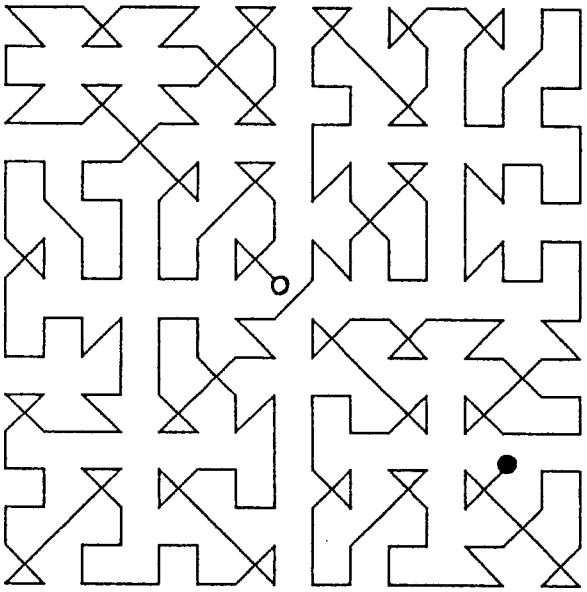
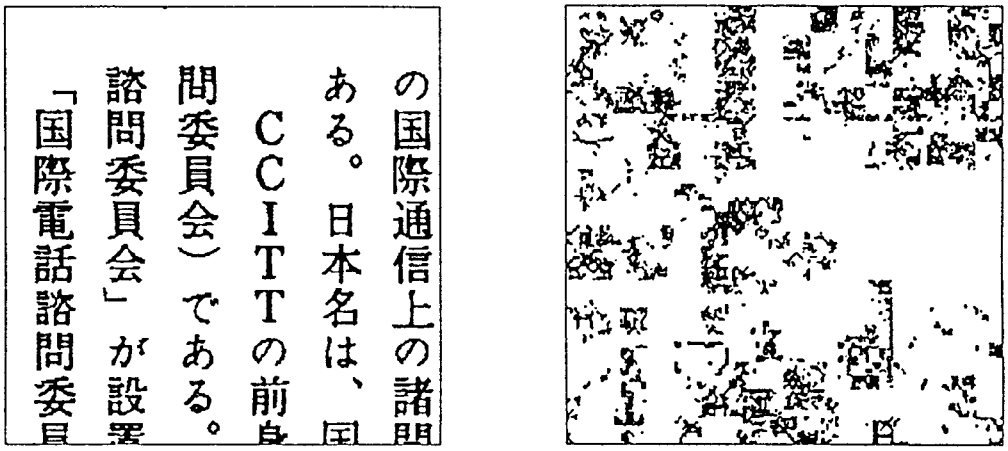


図2　ＩＳＦＣ走査例



(a)　原画像　　(b)　スクランブル画像

図3－1　多値画像

(a)　原画像　　(b)　スクランブル画像

図3－2　多値画像

図3　ＩＳＦＣスクランブル例

(3) スクランブルの評価

(a) スクランブル効果

ＳＮ比とともに主観評価を求めた。主観評価についは、木下等（東工大）の提案した５段階の判定基準であるＭＳＳ(Mean Security Score) を参考として、表１に示す判定基準を作成した。表１の判定基準に基づき、ＩＳＦＣ走査で文書画像に対してスクランブルを行なった評価結果を図４に示す。

表１　主観評価の判定基準

評点	判　定　基　準
5	画像の内容が分かる
4	一部分からないが、ある程度の内容は分かる
3	ほとんど分からないが、部分的には内容をつかめる
2	画像の内容は分からないが、その種類は分かる
1	何が書いてあるのかその種類すら分からない

（木下、塩入、酒井（東工大）が提案している５段階評価を参考）

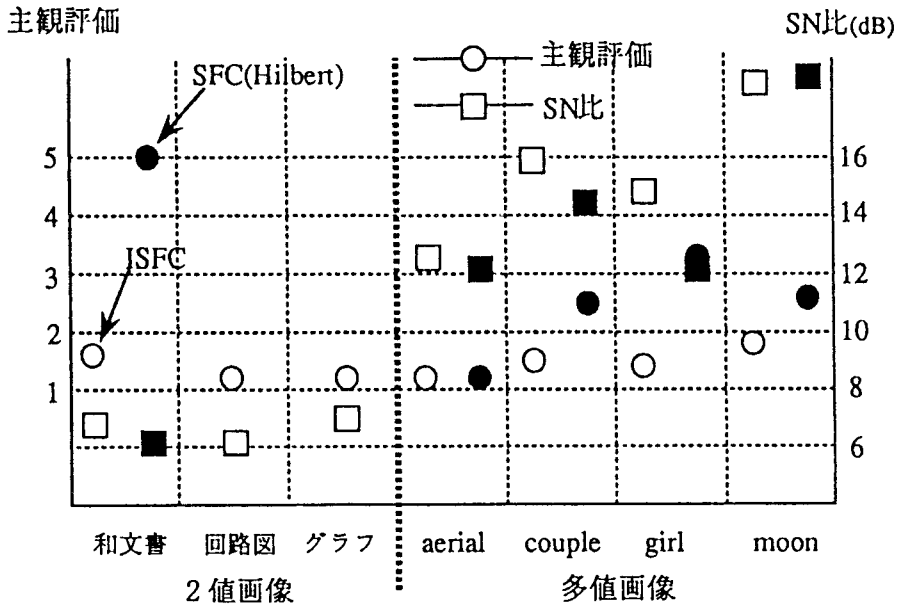


図４　ＩＳＦＣのスクランブル効果

図４より、ＩＳＦＣによりスクランブルを施した結果の主観評価値は、対象とした文書画像の種類に係わらず２以下となっており、情報の内容は分からないという結果が得られた。さらに本研究では、画像を複数の階層に分割し、各階層（もしくは一部）に対してＳＦＣ走査を施すスクランブル手法も提案しており[5]、ＩＳＦＣと組合せることによりスクランブル効果が一層高まるものと考えられる。

(b) スクランブル文書画像の符号量

ＩＳＦＣが Hilbert走査と比較してエントロピーが増加している理由は、ＩＳＦＣでは画素間を斜め方向に走査していることを許容している点が原因になっていると考えられる。特に、２値画像については増加の割合が約12%であり、多値画像の場合と比べて大きくなっている。また、文字図形情報（２値）の走査については、ＩＳＦＣのエントロピーがラスター走査と比較して16%程度増加している。この原因としては、文字・図形の境界線部分を走査することにより白画素／黒画素の孤立点が増加することが挙げられる。なお、この対策についてはフィルタ処理等の検討を進めている。多値画像をスクランブルした場合は、Hilbert走査と比較して２%程度の増加であり、２値の文書画像の場合と比べて増加の程度は少ない。

本研究では、①使用可能な鍵の数、解読の手間等に関する安全性評価、②符号化標準への適用、③ｎ（≧３）次元ＳＦＣを用いたスクランブルアルゴリズム、④映像情報への適用等が今後の課題として残されている。

3．文書画像通信における認証方式

(1) ディジタル透かしを用いた認証手段

画像の特徴を利用して文書等の信憑性を確保する一例に「透かし」がある。認証子を文書画像の中に丁度透かしのように埋め込む手法を「ディジタル透かし」と名付け[6]、ＩＣカードにディジタル透かしを適用した通信への適用に関する基本的な手法について提案を行なった[7]。
ディジタル透かしには、

① 透かし情報を取り除く等の不正を行なった場合、画像の品質が劣化する。
② 透かし情報は、許容できる画質が保たれる範囲内で画像に付加される。
③ 透かし情報の付加による符号量の増加は少ない。

の条件が必要とされている。透かしを実現する具体例として、これまで予測符号化を用いた手法を提案した[6]。

さらに本研究では、以上の研究成果を基に、２．で述べたＳＦＣを用いてディジタル透かしを実現する手法について考察を進めている。図５は、３次元ＳＦＣ走査を用いて認証子を表す１次元の符号系列（太線）を埋め込む概念図を示している。認証子を埋め込む対象しては、多値・カラー画像とともに映像情報等が考えられる。

(2) ＰＫＣＳ（Personal Key Cryptosystem）

通信システムの安全性を確保するためには、文書の信憑性とともに本人を正しく確認することも重要な課題の一つである。本研究では、指紋、音声、筆跡といった身体的特徴を用いて本人を確認する手段について提案する[8]-[10]とともに、通信に応用する手段に関する研究[11]を進めた。

さらに本研究では、文書画像の符号化手段と個人の特徴を抽出する手段に共通点があれば、抽出された個人の特徴パラメータをそのまま秘密鍵（個人鍵）として、文書画像の機密保護・認証通信に用いるシステム（ＰＫＣＳ（Personal Key Cryptosystem））を検討している。ここで、符

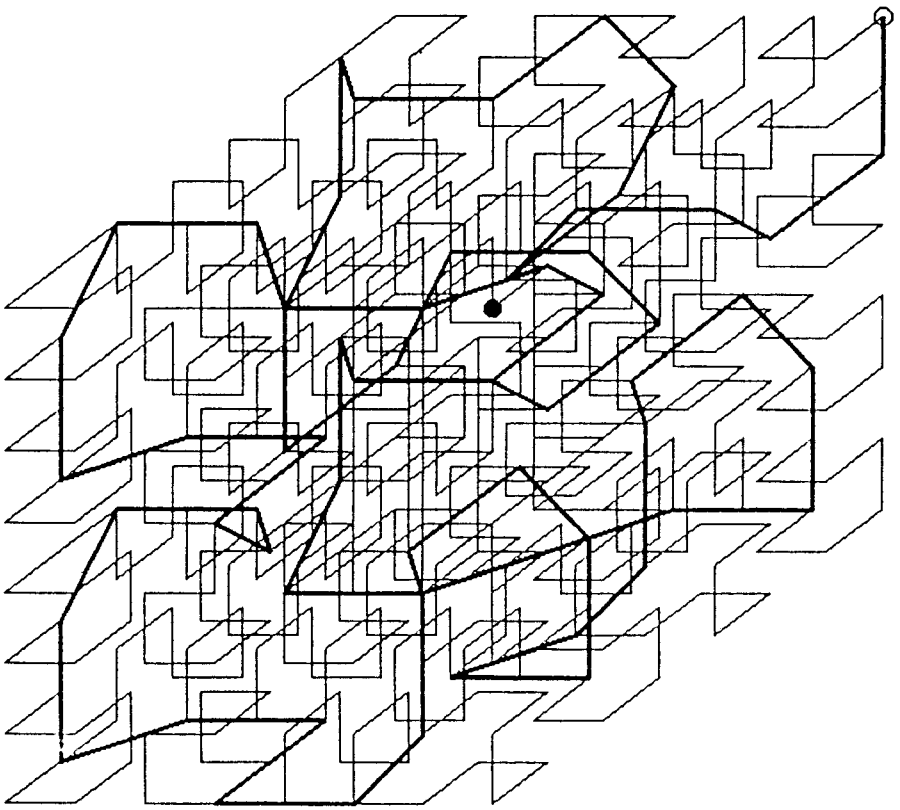


図5　3次元ＳＦＣを用いたディジタル透かしの実現手法

号化手段と個人の特徴の抽出手段の一つとして、ベクトル量子化を用いることが考えられ、筆跡情報を用いて基礎的な考察を行なった[8]。

ＰＫＣＳは個人の特徴を透かし情報とした「ディジタル透かし」の発展形と考えることができる。さらに指紋、音声等種々の個人の特徴を用いた研究課題が残されている。

5．おわりに

㈶髙柳記念電子科学技術振興財団の研究助成により進めた「文書画像情報の通信セキュリティに関する研究」の概要を述べた。文書画像通信に対するセキュリティのニーズは今後さらに高まるものと考えられ、本研究成果をもとに今後さらに研究を進めていきたい。

本研究成果は、㈶髙柳記念電子科学技術振興財団の多大なるご支援によるものであり、関係各位に深くお礼申し上げます。

参考文献

〔1〕小松：“ファクシミリにおけるセキュリティ技術”，画像電子学会誌，Vol.19，No.4，pp.229-235（1990）.

〔2〕佐藤、小松：“ＳＦＣを用いた文書画像のスクランブルアルゴリズム”，信学春季全大，D-442（1992）.

〔3〕小松、小宮山：“ＳＦＣを用いた文書画像のスクランブル手法”，SCIS92論文集，SCIS92-17D (1992-04).
〔4〕小松、小宮山：“ＳＦＣを用いた文書画像のスクランブル手法”，画像電子学会研究会講演予稿，92-02-05 (1992-09).
〔5〕小宮山、小松：“階層形ＳＦＣを用いた文書画像のスクランブル手法の提案”，信学春季全大，D-443 (1992).
〔6〕小松、富永：“文書画像通信におけるディジタル透かしの提案と署名への応用”，信学論（Ｂ－Ｉ），J72-B-Ｉ，3，pp.208-218 (1989-03).
〔7〕M.Yamada, N.Komatsu and H.Tominaga ：“Secure Document-image Management Facilities in Telematics ”, Proc. IWT (1989-09).
〔8〕小川、石渡、小松：“筆跡情報を用いた個人鍵の生成と個人識別手段”，信学春季全大，SA-8-3 (1991).
〔9〕武田、小松、木下、清水：“放射状走査を用いた指紋照合アルゴリズム”，信学春季全大，D-537 (1992).
〔10〕武田、小松、木下、清水：“放射状走査を用いた指紋照合アルゴリズムの提案”，SCIS92論文集，SCIS92-8D (1992-04).
〔11〕木下、清水、小松：“個人認証の適用領域とセキュリティレベルに関する一考察”，SCIS92論文集，SCIS92-8C (1992-04).