

要 旨

統計的性質に基づいた JPEG 2000 半開示画像への攻撃法

濱口 真伍

近年，ネットワークを利用した商品としてのデジタル画像の流通量が増加し，不正コピーによる著作権侵害が問題となっている．著作権保護の手法として，電子透かし，画像情報全体の暗号化，情報半開示が提案されている．電子透かしは，著作権情報を画像に埋め込み，不正コピーを抑止し著作権を保護する．しかし，電子透かしは画像の不正コピー自体を未然に防止することが困難である．画像情報全体の暗号化は，画像にノイズを付加し，画像の内容を見えなくする方式である．この方式は，画像の内容を保護するのに最も安全である．しかし，完全に復号しなければ画像の内容を確認できないので，画像内容の確認に手間がかかり検索に制約がある．

これに対して，画像の情報半開示は，商品として画像を流通させる著作権保護に有用な方式である．この方式は，画像に暗号を適用し，ユーザが画像に何が写っているか分かる程度にノイズを付加する．しかし，既存の情報半開示法においては，ウェーブレット変換の特徴から，半開示画像を復元される危険がある．

本論文では，ウェーブレット変換の特徴を用いた攻撃法を提案する．提案した攻撃法を半開示画像に適用し，ノイズ量の測定を行う．測定結果から，本手法が著作権保護に有効であることを示す．

キーワード JPEG 2000，情報半開示，ウェーブレット変換

Abstract

Cryptanalysis JPEG 2000 partial scrambled images based on statistical character

Shingo HAMAGUCHI

In recent years, distributions of commercial digital images using network increases and copyright piracy becomes problems by unauthorized copying. Methods of copyright protection are proposed digital watermarking, encryption of image and partial-scrambling. Digital Water Marking is suggested as a method of copyright protection. Digital Water Marking embeds copyright notice in digital image and prevent unfair use. Though this method is difficult to prevent unfair use. Encryption of image is the safest method in protection of image information. However we cannot confirm image content without completely decrypting image information and this method disturbs treatment of image and image search.

Consequently partial-scrambling of image is an useful method which protects copyright if commercial digital images are distributed. This method makes images deteriorate by using encryption and users can recognize image outline. However an existing partial-scrambling is in danger of being restored scrambled images by a feature of image frequency transform.

In this article, we point problems of an existing partial-scrambling and approach a cryptanalysis. Additionally we perform simulation and determines image noise. Then we confirm an effect of cryptanalysis.

key words JPEG 2000, Partial-Scrambling, DWT