

モーフィングに基づく顔画像の隠蔽技術 ～秘密情報を隠しても画像は自然～

教授 趙 強福



データを集める前に、まずプライバシーを考えましょう

概要

- データ隠蔽技術として昔からステガノグラフが知られている。ステガノグラフでは秘密情報はカバーデータの中に隠すことによって保護される。カバーデータとして、通常、画像、音楽などを利用する。秘密情報を隠すときに、カバーデータの「外観」をあまり変えないようにしておけば、第三者は秘密情報の存在すら知り得ないので、ステガノグラフは暗号化技術よりも「攻撃」される可能性は低いと言われている。
- 問題点としては、「カバー率」が低いことが挙げられる。即ち、顔画像などのような情報量の大きい情報を隠そうとする場合、従来の方法ではカバーデータの情報量も大きくなり、効率的でない。
- 本技術では以上の問題点を克服し、顔画像などを効率よく隠蔽することができる。



※左から順に、隠したい画像、カバー画像、モーフィング画像である。モーフィング画像が公開されても「あるヒト」の顔として認識され、元の人個人情報が保護される。鍵を持っている者だけが元の画像を復元することができる。

実用化の可能性

- 本技術は、
 - 1) 一枚の画像を隠すために、同サイズの2枚の画像といくつかのパラメータで十分であり、従来方法よりカバー率が高い。
 - 2) 一部の情報(顔の属性など)を隠しつつ、他の情報(顔色、表情など)が公開できる。などの特徴がある。
- 本技術は、さまざまな顔画像データベースに含まれる大事な個人情報を守ることができる。データベースの例として、顔認証による入室管理システム、顔画像によるセキュリティシステムなどを構築する際に使う訓練データベースが挙げられる。

UBICからのメッセージ

- モーフィングとは画像を連続的に変形する、という意味です。この技術によれば、顔画像を隠蔽する際、従来技術に比べカバー画像の情報量が少なくても良い、という利点があります。
- 高いセキュリティを保証する方法として顔認証があり、この場合顔画像は重要な個人情報ですが、顔認証のための顔画像が流出したら影響は測り知れません。
- 銀行、クレジットカード会社等高いセキュリティが要求される所での本技術の応用が期待されます。

研究概要図

