視覚暗号の研究

視覚暗号は、1995 年に、Naor と Shamir によって提案されました。暗号化は、図１のような秘密画像を、２つのランダムな画像Ａ，Ｂに分散符号化し、Ａをアリスに、Ｂをボブに渡すことにより行われます。

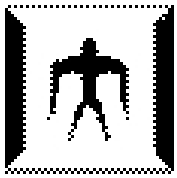

図１．元の秘密画像

復号化は、非常に簡単です。アリスとボブは、分散画像ＡとＢを単に重ね合わせることにより、図２のような画像を復元するわけです。暗号の何らかの知識、あるいはソフトウェア、ハードウェア等を全く必要としません。これが、高度に専門的な知識、および高性能な計算機を必要とする、一般の現代暗号との違いです。

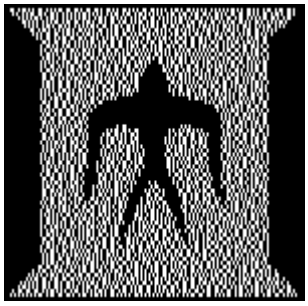

図２．従来の復元画像

しかし、図２からわかるように、コントラストが大幅に劣化してしまうのが、従来の方式の欠点です。これは、分散画像Ａ，Ｂにおける黒いピクセルは、決して白にはできないからです。（復号は、２つの分散画像を単に重ね合わせるだけなので。）

これに対し、我々は、コピー機の白黒反転機能を利用することにより、元画像をほぼ完全に復元する方法を開発しました。提案方式による復元画像を図３に示します。

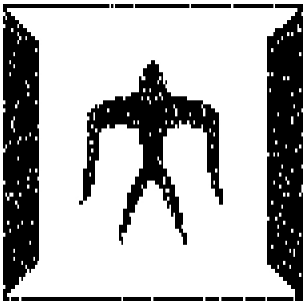

図３．提案方式による復元画像

さらに、本方式をカラー画像に拡張する方法も、開発しています。

参考文献・著書・特許等:
特願 2004-15645

教員名：黒澤　馨（茨城大学工学部情工学科教授）
TEL：0294-38-5135　FAX：0294-38-5135　E-mail：kurosawa@cis.ibaraki.ac.jp
URL：http://kuro.cis.ibaraki.ac.jp/~kurosawa/KuroIwa.htm