ユーザ特性を活用した情報セキュリティ技術の開発

Keyword : 情報セキュリティ、システムセキュリティ、コンテンツ保護、ユーザ認証

研究の概要

1）画像変調方式によるコンテンツ保護

暗号技術によって、復号鍵を持っている購入者にのみコンテンツを配信することは可能であるが、購入者自身が悪意を持っていた場合、購入者の手元からコンテンツが流出することになる。この問題に対処するには、購入者の手元でさえコンテンツが復号されることはなく、しかし、購入者にはコンテンツの視聴を許す必要がある。

画像変調方式は、不完全ながら、「どこにも本物のコンテンツが存在しないのに、ユーザにそのコンテンツを知覚させる」ことができる方式である（図1）。

配信者は、まず、オリジナル画像を複製して2枚（画像1，2）にする。次に、画像1に対しては輝度レベルを＋α、画像2に対しては－αすることにより、変調画像1，2を作成する。ここで、αは画像の変調量であり、各画素ごとに独立な値を選ぶことが可能である。購入者には、変調画像1，2を配信する。

購入者は、専用のプログラムを使用して2数の変調画像を高速に切替表示する（図2）だけである。切り換えの速度がおよそ100Hzを超えてくると、継時加法混色と呼ばれる人間の視覚特性が働き、＋αの変調と－αの変調が打ち消されて変調をかける前のオリジナル画像とほぼ同画質の画像が知覚される。しかし、実際に表示されている画像は変調画像1または2であり、オリジナル画像はどこにも存在しない。

2）画像認証方式の強化

記憶情報によるユーザ認証方式の主流はパスワード認証であるが、人間にとって長くランダムな文字列を記憶することは容易ではない。そのため、人間の画像認識能力の高さを利用して記憶負荷を低減させる画像認証方式が注目されている。しかし、この画像認証方式の長所が、「毎回の認証時にパス画像が画面上に表示されるがゆえに、認証時の覗き見攻撃に対する耐性を保てない」という新たな脆弱性を生み出してしまっていた。

画像認証方式にとって覗き見攻撃が脅威となるのは、正規ユーザのみならず覗き見攻撃者にとっても画像の記憶が容易であるからである。そこで、覗き見攻撃者にとってパス画像の記憶が困難となるように、モザイク化等の不鮮明化処理を施した一見無意味な画像（以下、不鮮明化画像）をパス画像として使用する。人間は画像の記憶に優れているという特性を有するものの、それは有意味な画像を記憶する場合に限ってのことであり、無意味に見える（意味を言語化できない）画像を記憶することはやはり難しい。ゆえに、他人のパス画像（不鮮明化画像）を覗き見て記憶することは、攻撃者にとって困難な作業となる。

正規ユーザにのみ、パス画像の登録時に不鮮明化処理を施す以前の有意味なオリジナル画像を見せ、当該画像に不鮮明化処理を施したパス画像と合わせて記憶してもらうようにする。不鮮明化画像にはオリジナル画像の特徴がある程度残されているため、オリジナル画像を見ることによって、正規ユーザは不鮮明化画像を有意味な画像として認識できるようになり、パス画像を容易に記憶することができる（図3）。

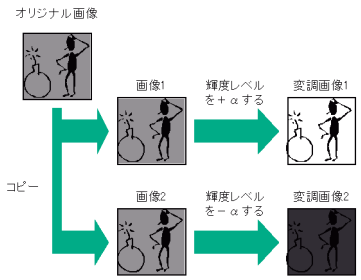

図 1. 画像変調

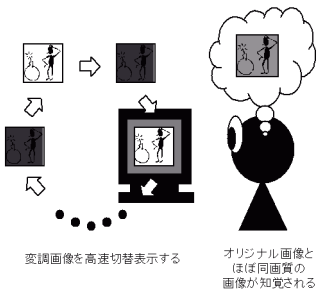

図 2. 変調画像の高速切替表示

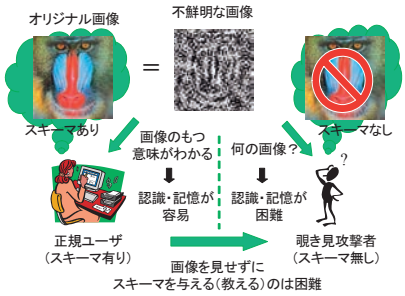

図 3. 不鮮明化画像を利用した画像認証方式

■ 技術相談に応じられる関連分野

・情報セキュリティ全般

皆様との産学連携によって、新たなイノベーションの創出を期待しています！

西垣　正勝

創造科学技術大学院
教授