A New Rule for Cost Reassignment in Adaptive Steganography

ABSTRACT

Steganography is a technique for covert communication, which aims to hide secret messages into ordinary digital media without drawing suspicion. Designing steganographic algorithms for various cover sources is challenging due to the fundamental lack of accurate models. Currently, the most successful approach for designing content adaptive steganography is based on minimizing the distortion between the cover and the corresponding stego object.

EXISTING SYSTEM

In Existing System, Steganography schemes, the distortion function is used to define modification costs on cover elements, which is distinctly vital to the security of modern adaptive steganography. There are several successful rules for reassigning the costs defined by a given distortion function, which can promote the security level of the corresponding steganographic algorithm.

DIS ADVANTAGES

- Texture complexity will no longer promote the security of steganography.
- Weakening the performances of adaptive steganalysis and promoting the security of steganography.

PROPOSED SYSTEM

In Proposed System, we propose a novel cost reassignment rule which is applied to not one but a batch of existing distortion functions. We find that the costs assigned on some pixels by several steganographic methods may be very different even though these methods exhibit close security levels. We call such pixels *"controversial pixel"*. Experimental results show that steganalysis features are not sensitive to controversial pixels, therefore these pixels are suitable to carry more payloads. We name this rule the Controversial Pixels Prior (CPP) rule. Following the rule, we propose a cost reassignment scheme. Through extensive experiments on several kinds of stego algorithms, steganalysis features and cover databases, we demonstrate that the

CPP rule can improve the security of state-of-the-art steganographic algorithms for spatial images.

ADVANTAGES

- To find controversial pixels by comparing several comparable steganographic methods.
- To achieve a prominent increase in security.

SYSTEM REQUIREMENTS

H/W System Configuration:-

Processor	-	Pentium –III
RAM	-	256 MB (min)
Hard Disk	-	20 GB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

S/W System Configuration:-

Operating System	:	Windows95/98/2000/XP
Application Server	:	Tomcat5.0/6.X
Front End	:	HTML, Jsp
Scripts	:	JavaScript.
Server side Script	:	Java Server Pages.
Database	:	MySQL 5.0
Database Connectivity	:	JDBC