**Title:** **Hybrid model for Text & Image encryption**

**Abstract:** Security is major concern in data handling, communication and message transmission on public network. Cryptography is the encryption process of transformation of messages to make information secure and resistant to attack. AES is symmetric encryption standard recommended by NIST. AES is proved to be highly secure, faster and strong encryption algorithm. But in recent years cyber-attacks are continuously developing, therefore security specialists must stay busy in the lab inventing new schemes to keep attackers at bay. Possible attacks on symmetric algorithm can be Brute-force Attack, Differential Attack, Algebraic Attack and Linear Attack. So, to provide strong security in message transmission, AES algorithm with Diffie-Hellman Key exchange algorithm and steganography is proposed.

**Block diagram**

client server

public key public key

Diffie-hellman key exchange

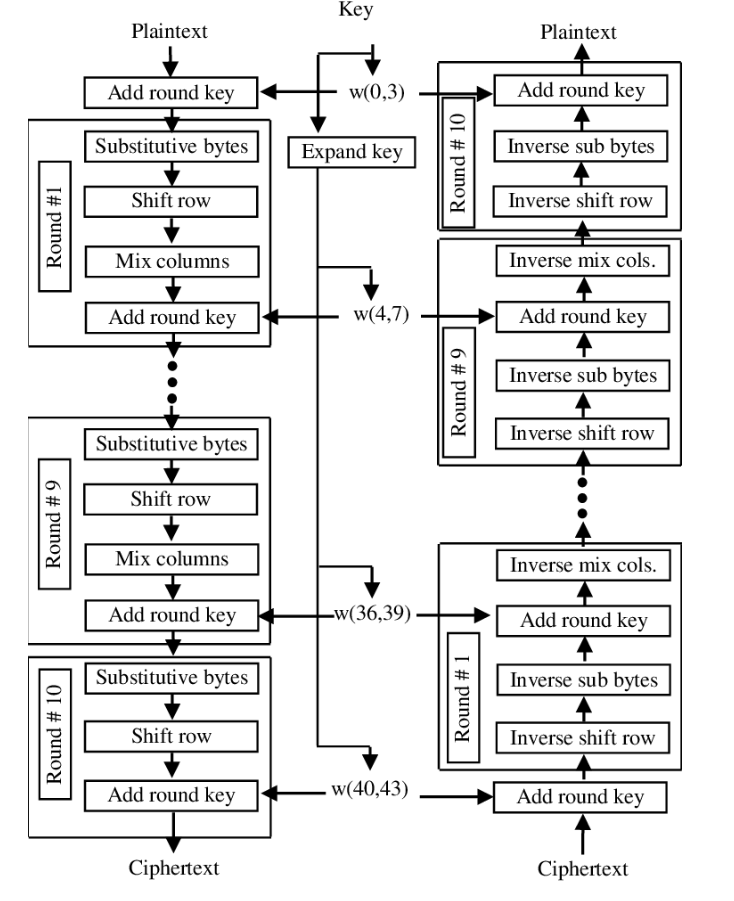
Private value

Private value

Shared secret key

Shared secret key

Shared secret key



steganography

Communication channel

Stego-key

cover medium

Stego-key

Cover medium

Extracting process

Embedding process

Shared key