

METHOD AND APPARATUS FOR **DIGITAL CONTENT COPY PROTECTION**

Abstract

A method, apparatus and a computer program product are described for copy protecting encrypted documents in a client-server system using an unsecured communication channel. The client-server system has clients (16) and a server (12) for storing encrypted documents. Encrypted documents $e(K_s, M)$ are received by a client (16) from the server (12). Communications on a transmission channel (14) between the client (16) and the server (12) are then authenticated. Such communications also include electronic payments initiated by a user using the client (16). Upon authenticating or payment, an encrypted document can then be decrypted. After decrypting, the unencrypted document is displayed but prevented from storage at any client (16) unless re-encrypted using a host specific key K_H associated with the client (16) to thereby provide a re-encrypted document.

FIG. 4 accompanies this abstract.