



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) Publication number : **0 644 474 A1**

(12)

EUROPEAN PATENT APPLICATION

(21) Application number : **94306679.5**

(51) Int. Cl.⁶ : **G06F 1/00, G11B 20/00**

(22) Date of filing : **12.09.94**

(30) Priority : **13.09.93 US 120969**

(43) Date of publication of application :
22.03.95 Bulletin 95/12

(84) Designated Contracting States :
DE GB

(71) Applicant : **NATIONAL UNIVERSITY OF SINGAPORE**
Heng Mui Keng Terrace,
Kent Ridge
Singapore 0511 (SG)

(72) Inventor : **Arcot Desai, Narasimhalu**
9 Ross Avenue
Singapore 1129 (SG)
Inventor : **Wang, Weiguo**
103 Jalan Hitam Manis
Singapore 1027 (SG)
Inventor : **Kankanhalli, Mohan Shankara**
74 Jalan Hitam Manis
Singapore 1027 (SG)

(74) Representative : **Driver, Virginia Rozanne et al**
Page White & Farrer
54 Doughty Street
London WC1N 2LS (GB)

(54) **A method for utilising medium nonuniformities to minimize unauthorized duplication of digital information.**

(57) The present invention is a method for preventing unauthorized copying and use of information which is stored on a storage medium and for restricting the use of such information to designated devices. Copy protection is achieved by generating a signature from a given storage medium. The signature is derived from an arbitrarily selected list of nonuniformities, uniformities and their attributes. The selected list may contain nonuniformities at any granularity level. As such, this signature is unique to a given storage medium in the same way finger prints are unique to a human being. This signature is used to derive a key for encrypting the information on the storage medium. Any copying of the distribution information from one storage medium to another results in the mutation of the signature required to decrypt the information. Therefore, the present invention obviates the need for introducing artificial indicia or requiring a special hardware subsystem for achieving a copy protection scheme.

Restricting the usage of information on a distribution medium to a designated device is achieved by verifying the device ID (DID-D) of the device with the device ID (DID-S) stored in the distribution medium before the decryption and transfer of information are undertaken. Decryption of the information is accomplished by generating a key from both the signature of the distribution medium and the DID-S.

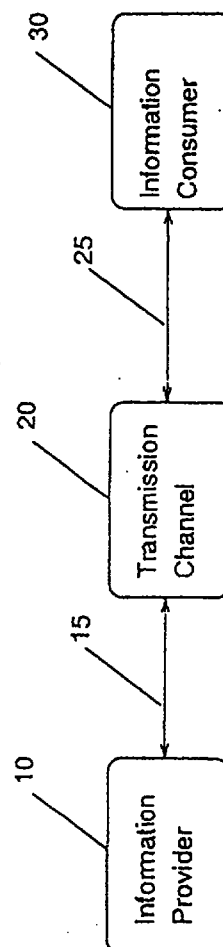


Figure 1

EP 0 644 474 A1

REPLACED SHEETS		SG
☒	Description	: paged 2 to paged 4
☒	Claim(s)	: paged 6 to paged 7
☒	Drawing(s)	: paged 5 to paged 14
☒	Abstract	: paged 1 to paged 1
DATE OF RECEIPT		

Jouve, 18, rue Saint-Denis, 75001 PARIS

This Sheet Has Been Replaced

