PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04N 7/167

A1

(11) International Publication Number: WO 97/35431

(43) International Publication Date: 25 September 1997 (25.09.97)

(21) International Application Number: PCT/GB97/00697

(22) International Filing Date: 13 March 1997 (13.03.97)

(30) Priority Data:
9605472.1 15 March 1996 (15.03.96) GB

(71) Applicant *(for all designated States except US)*: DIGI-MEDIA VISION LIMITED [GB/GB]; 1 Heathrow Boulevard, 286 Bath Road, West Drayton, Middlesex UB7 0DQ (GB).

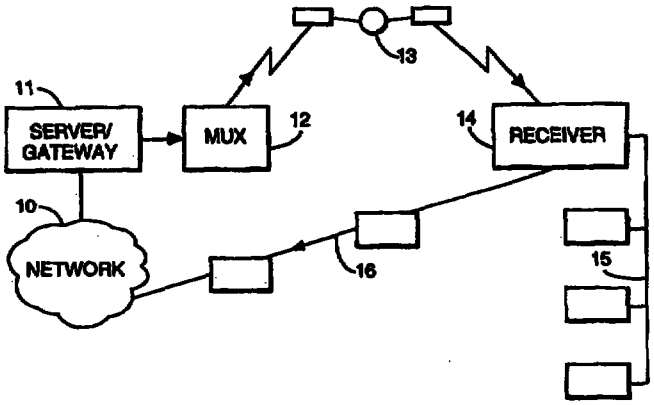
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: DALLARD, Nigel, Stephen [GB/GB]; 17 Lyddiard Close, Boyatt Wood, Eastleigh, Hampshire SO50 4NW (GB). GOLD, Martin [GB/GB]; Bramble Cottage, Lynton Meadow, Chilbolton, Stockbridge, Hampshire SO20 6BE (GB). MERRY, Paul, Austin [GB/GB]; 14 Shepherds Close, Bartley, Southampton, Hampshire SO40 2LJ (GB). MOUNTIFIELD, Anthony [GB/GB]; 6 Sawyers Close, Winchester, Hampshire SO22 5JX (GB).

(74) Common Representative: DIGI-MEDIA VISION LIMITED; Attn: Anderson, Angela, Mary, Stoneham Rectory, Stoneham Lane, Eastleigh, Hampshire SO50 9NW (GB).

(81) Designated States: AU, BR, CA, CN, IL, JP, KP, KR, MX, NO, NZ, SG, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: SECURE DATA BROADCASTING



(57) Abstract

The invention relates to a method and apparatus for protecting the destination addresses of data being transmitted over a digital video broadcasting channel. If the destination addresses are clear (i.e. not encrypted), it is possible for the traffic of data being transmitted to receivers subscribing to the channel to be monitored, and commercial information relating to this traffic may consequently be exposed. The invention provides that the destination addresses are encrypted by calculation from a sequence of control words. The video signal also includes entitlement control messages (ECMs) which include the control words in encrypted form. An address flag is associated with each destination address and a control flag is associated with each control word. At each receiver, the ECMs are processed to construct receiver addresses by calculation from the received control words and a unique receiver identifier. The receiver has two address registers for the calculated addresses referred to as odd and even. If the control flag for an ECM indicates odd, the calculated receiver address is registered to update the odd receiver address. If the control flag for an ECM is even, the calculated receiver address is registered to update the even receiver address. The address flags are also designated odd or even and determine which receiver address each destination address is compared with. Thus, each receiver has two dynamic addresses, one being in use and the other being updated at any one time.