PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :	A3	(11) International Publication Number:	WO 99/10859
H04L 9/06		(43) International Publication Date:	4 March 1999 (04.03.99)

(21) International Application Number: PCT/US98/17839

(22) International Filing Date: 28 August 1998 (28.08.98)

(30) Priority Data:

08/919,198	28 August 1997 (28.08.97)	US
08/919,212	28 August 1997 (28.08.97)	US
08/919,366	28 August 1997 (28.08.97)	US
08/919,203	28 August 1997 (28.08.97)	US

(71) Applicant: SYNDATA TECHNOLOGIES, INC. [US/US]; West Building, 500 Frank W. Burr Boulevard, Teaneck, NJ 07666 (US).

(72) Inventor: ORRIN, Steven, M.; 43 Conforti Avenue #77, West Orange, NJ 07052 (US).

(74) Agents: KOCH, Robert, J. et al.; Fulbright & Jaworski L.L.P., 801 Pennsylvania Avenue N.W., Washington, DC 20004 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

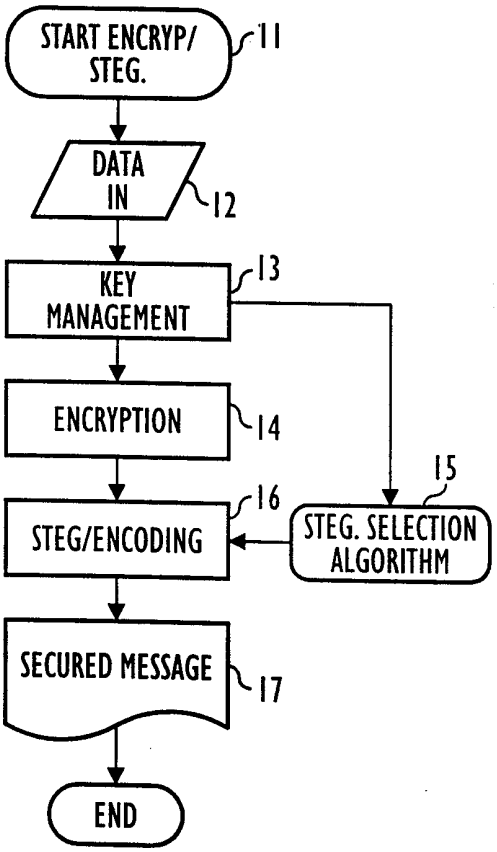
Published
With international search report.

(88) Date of publication of the international search report:
17 June 1999 (17.06.99)

(54) Title: STEGANOGRAPHIC ENCRYPTION SYSTEM FOR SECURE DATA

(57) Abstract

A data security system for digitized data that can use both encryption and steganographic techniques. Encrypted data (14) is steganographically encoded into a secondary data stream (16), the least significant bit of selected bytes of which are replaced with bits of the encrypted data. Byte selection (15) is performed via ciphertext created separately that uses an encryption key (13) as both key and data to be encrypted. The resulting secondary data stream (17) chosen such that it does not resemble any modification can be stored or transmitted. Decoding is accomplished by using the cypertext to find the selected bytes in the modified secondary data stream, extracting the least significant bits, and reassembling those bits into the original data. Data can be backed up by first encrypting it, then splitting it into multiple parts and storing each part on separate floppy disks in locations selected by separate encryption process which produces a selection ciphertext. The original data is restored by merging the data blocks from each floppy.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/17839

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) : H04L 9/06
US CL : 380/42
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/4, 5, 37, 42, 45; 382/284; 711/114, 153, 161, 162

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Please See Extra Sheet.

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, INSPEC, IAC, DERWENT, JAPIO, DIALOG, DR-LINK, IEL, PROQUEST DIRECT

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	US 5,778,074 A (GARCKEN et al.) 07 July 1998 (07.07.98), col. 4, lines 63-67, col. 5, lines 1-5, 51-56, col. 6, lines 2-12, 43-51, col. 11, lines 59-60, col. 12, lines 1-6, figure 1, items 14, 15 and 16.	1, 2, 7, 10, 11, 12, 17, 20, 21, 22, 27, 30, 31, 32, 37
Y,P		3, 4, 5, 13, 14, 15, 23, 24, 25, 33, 34, 35, 42, 46, 50, 54, 57, 59-63, 65-68
Y	WAYNER, P. Digital Copyright Protection, Academic Press, June 1996, pages 122-126, especially pages 122-123.	3, 13, 23, 33

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
04 MARCH 1999

Date of mailing of the international search report
23 MAR 1999

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
JUSTIN T. DARROW
Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/17839

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 5,745,569 A (MOSKOWITZ et al.) 28 April 1998 (28.04.98), col. 6, lines 9-13.	4, 14, 24, 34
Y	US 5,613,004 A (COOPERMAN et al.) 18 March 1997 (18.03.97), col. 3, lines 32-36, 49-53.	5, 15, 25, 35
X,E ---- Y,E	US 5,850,522 (WLASCHIN) 15 December 1998 (15.12.98), col. 2, lines 48-52, 60-62, col. 6, lines 20-24.	41, 43, 48, 49, 51, 56 ---- 42, 44-47, 50, 52-55
Y,E	US 5,860,090 A (CLARK) 12 January 1999 (12.01.99), col. 4, lines 59-67, col. 6, lines 20-45, figure 3, step 102.	44-47, 52-55
Y,E	US 5,832,523 A (KANAI et al.) 03 November 1998 (03.11.98), col. 7, lines 61-66.	47, 55
X	SZEPANSKI, W., A Signal Theoretic Method for Creation Forgery-Proof Documents for Automatic Verification. May 1979 Carnahan Conference on Crime Countermeasures, pp. 101-109, especially page 103.	57, 59-63, 65-72
A,P	US 5,737,417 A (BUYNAK et al.) 07 April 1998 (07.04.98), col. 1-3, col. 4, lines 1-47.	1-40
A,P	US 5,748,783 A (RHOADS) 05 May 1998 (05.05.98), col. 1, lines 1-63.	1-40
A,E	US 5,838,796 A (MITTENTHAL) 17 November 1998 (17.11.98), col. 1, col. 2, lines 1-36.	1-40
A,E	US 5,802,174 A (SAKO et al.) 01 September 1998 (01.09.98), col. 2, lines 58-67, col. 3, lines 1-2.	47, 55
A,E	US 5,875,477 A (HASBUN et al.) 23 February 1999 (23.02.99), col. 1, col. 2, lines 1-37.	41-56

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/17839

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/17839

B. FIELDS SEARCHED
Documentation other than minimum documentation that are included in the fields searched:

WAYNER, P., Digital Copyright Protection. Academic Press, June 1997
SCHNEIER, B., Applied Cryptography. John Wiley & Sons, Inc., 1996

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single inventive concept under PCT Rule 13.1. In order for all inventions to be searched, the appropriate additional search fees must be paid.

Group I, claim(s)1-20, drawn to steganography system for secure data.
Group II, claim(s) 21-40, drawn to combined encryption and steganography system for secure data.
Group III, claim(s) 41-56, drawn to data backup using encryption and steganography.
Group IV, claim(s) 57-68, drawn to encryption-based selection system for steganography.

The inventions listed as Groups I, II, III and IV do not relate to a single inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of Group I is the technique of steganography of data claimed while the special technical feature of Group II is the.