(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年9 月1 日 (01.09.2005)

PCT

(10) 国際公開番号
WO 2005/081450 A1

(51) 国際特許分類[7]: H04L 9/08, 9/32

(21) 国際出願番号: PCT/JP2004/019713

(22) 国際出願日: 2004 年12 月22 日 (22.12.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-48457 2004 年2 月24 日 (24.02.2004) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 佐藤 英雄 (SATO,Hideo) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

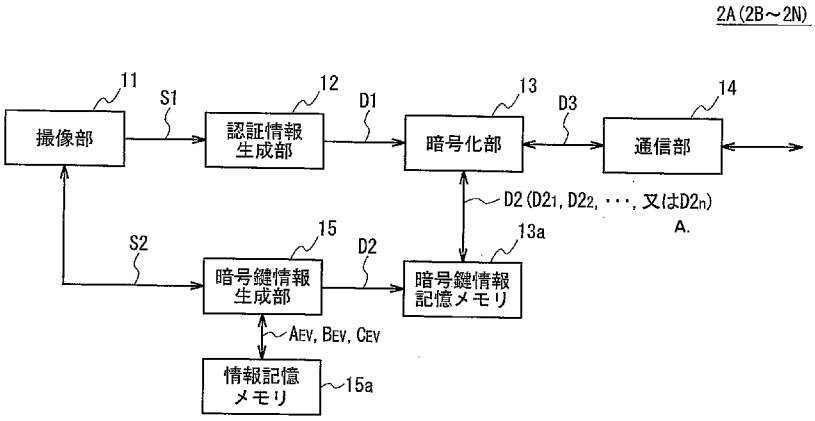
(74) 代理人: 田辺 恵基 (TANABE,Shigemoto); 〒141-0032 東京都 品川区 大崎３丁目６番４号 トキワビル５階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[続葉有]

(54) Title: ENCRYPTING APPARATUS AND ENCRYPTING METHOD

(54) 発明の名称: 暗号化装置及び暗号化方法



11.. IMAGING PART
12.. AUTHENTICATION INFORMATION PRODUCING PART
13.. ENCRYPTION PART
14.. COMMUNICATION PART
A.. D2 ($D2_1$, $D2_2$, ..., OR $D2_n$)
15.. ENCRYPTION KEY INFORMATION PRODUCING PART
15a.. INFORMATION STORAGE MEMORY
13a.. ENCRYPTION KEY INFORMATION STORAGE MEMORY

(57) Abstract: An encrypting apparatus and an encrypting method wherein the reliability of an encrypting function can be improved. A parameter specific to a solid-state imaging element is produced based on a uniform image signal (S2) outputted, from the solid-state imaging element, as an imaging result of a uniform subject in an imaging part (11). Encryption key information (D2) derived from the foregoing specific parameter is used to encrypt authentication information (D1). In this way, the concealment of the authentication information (D1) can be easily and simply maintained, so that the reliability of the encryption function can be improved.

(57) 要約: 暗号機能の信頼性を向上し得る暗号化装置及び暗号化方法を提案する。撮像部11における均一な撮像対象の撮像結果として固体撮像素子から出力される均一画像信号S2に基づいて当該固体撮像素子固有の素子

[続葉有]

WO 2005/081450 A1

SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

固有パラメータを生成し、この素子固有パラメータから導出した暗号鍵情報D2を用いて認証情報D1を暗号化するようにしたことにより、認証情報D1の秘匿性を簡易に確保することができ、かくして暗号機能の信頼性を向上することができる。