

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TRANSCEND INFORMATION INC.,

Petitioner,

v.

TRUESIGHT COMMUNICATIONS LLC,

Patent Owner.

Case: IPR2024-00723
U.S. Patent No. 8,977,783

DECLARATION OF R. JACOB BAKER, PH.D., P.E.

IN SUPPORT OF PETITION FOR

***INTER PARTES* REVIEW OF U.S. PATENT NO. 8,977,783**

I. INTRODUCTION

1. My name is R. Jacob Baker Ph.D., P.E., and I am a professor emeritus of electrical and computer engineering at the University of Nevada, Las Vegas (“UNLV”). I have prepared this declaration as an expert witness on behalf of Petitioner Transcend Information Inc. In this declaration, I provide my opinions regarding the validity of claims 1-18 (the “Challenged Claims”) of U.S. Patent No. 8,977,783 (“the ’783 Patent”) (Ex. 1001). I also provide herein the technical bases for these opinions, as appropriate.

2. This declaration contains statements of my opinions formed to date, and the bases and rationale for these opinions. I may offer additional opinions based on further review of materials in this case, including opinions and/or testimony of other expert witnesses.

3. For my efforts in connection with the preparation of this declaration, I have been compensated at my usual and customary rate for this type of consulting activity. My compensation is in no way contingent on the results of these or any other proceedings related to the ’783 Patent.

a. Qualifications / Professional Background

4. My qualifications generally are set forth in my Curriculum Vitae, which is included as Ex. 1004. Ex. 1004 also includes a list of the publications I have

authored and a list of the other cases in which I have testified during the last four years.

5. I have been working as an engineer since 1985, and I have been teaching Electrical and Computer Engineering courses since 1991.

6. I received B.S. and M.S. degrees in Electrical Engineering from UNLV in 1986 and 1988, respectively. I received my Ph.D. in Electrical Engineering from the University of Nevada, Reno (“UNR”), in 1993.

7. My doctoral research, culminating in the award of a Ph.D., investigated the use of power MOSFETs in the design of very high peak power, and high-speed, instrumentation. I developed techniques to reliably stack power MOSFETs to switch higher voltages, that is, greater than 1,000 V and 100 Amps of current with nanosecond switching times. This work was reported in the paper entitled “Transformerless Capacitive Coupling of Gate Signals for Series Operation of Power MOSFET Devices,” published in the IEEE Transactions on Power Electronics. The paper received the Best Paper Award in 2000.

b. Industry Experience

8. From 1985 to 1993, I worked for EG&G Energy Measurements and the Lawrence Livermore National Laboratory designing nuclear diagnostic instrumentation for underground nuclear weapon tests at the Nevada test site. During this time, I designed, and oversaw the fabrication of, over 30 electronic and

electro-optic instruments, including high-speed cable and fiber-optic receiver/transmitters, PLLs, frame and bit-syncs, data converters, streak-camera sweep circuits, Pockel's cell drivers, micro-channel plate gating circuits, charging circuits for battery backup of equipment for recording test data, and analog oscilloscope electronics.

9. My work during this time, as one example, had a direct impact on my doctoral research work using power MOSFETs, subsequent publishing efforts, and industry designs. In addition to the 2000 Best Paper Award from the IEEE Power Electronics Society, I published several other papers in related areas while working in industry. I hold a patent, U.S. Patent No. 5,874,830, in the area of power supply design, titled, "Adaptively Biased Voltage Regulator and Operating Method," which was issued on February 23, 1999. I have designed dozens of linear and switching power supplies for commercial products and scientific instrumentation.

10. I am a licensed Professional Engineer and have extensive industry experience in circuit design, fabrication, and manufacture of Dynamic Random Access Memory (DRAM) semiconductor integrated circuit chips, Phase-Change Random Access Memory (PCRAM) chips, and CMOS Image Sensors (CISs) at Micron Technology, Inc. ("MTI") in Boise, Idaho. I spent considerable time working on the development of flash memory chips while at MTI. My efforts resulted in more than a dozen patents relating to flash memory. One of my projects

at MTI included the development, design, and testing of circuit design techniques for a multi-level cell (MLC) flash memory using signal processing. This effort resulted in higher-density memories for use in solid-state drives and flash memory cards having an ATA interface that are ubiquitous in consumer electronics, including cameras and data storage systems. This included both secure and non-secure storage systems. Further, the use of higher-density memory can result in fewer changes in the flash translation layer for logical-to-physical addressing, less need for garbage collection, and larger data segments that can improve a computing system's performance. Another project I worked on at MTI focused on the design of buffers for high-speed double-data rate DRAM, which resulted in around 10 U.S. patents in buffer design. Among many other experiences, I led the development of the delay locked loop (DLL) in the late 1990s so that MTI DRAM products could transition to the DDR memory protocol, used in mobile and non-mobile (server, desktop, cell phones, tablets, etc.) computing systems as main computer memory, for addressing and controlling accesses to memory via interprocess communications (IPC) with the memory controller (MC). I provided technical assistance with MTI's acquisition of Photobit during 2001 and 2002, including transitioning the manufacture of CIS products into MTI's process technology. Further, I did consulting work at Sun Microsystems and then Oracle on the design of memory modules during 2009 and 2010. This work entailed the design of low-power, high-speed, and wide

interconnection methods with the goal of transmitting data to/from the memory module and the MC at higher speeds.

11. I have extensive experience in the development of instrumentation and commercial products in a multitude of areas including: integrated electrical/biological circuits and systems, array (memory, imagers, and displays) circuit design, CMOS analog and digital circuit design, diagnostic electrical and electro-optic instrumentation for scientific research, CAD tool development and online tutorials, low-power interconnect and packaging techniques, design of communication/interface circuits (to meet commercial standards such as USB, firewire, DDR, PCIe, SPI, etc.), circuit design for the use and storage of renewable energy, and power electronics. For example, a part of my research at Boise State, for many years, focused on the use of Thru-Silicon-Vias (TSVs), aka Thru-Wafer Vias (TWVs), for high-density 3D packaging. These packaging techniques were utilized in the memory module development work I did with Sun Microsystems and Oracle. As another example, I designed circuitry for use in implementing Universal Serial Bus (USB) interface circuits while I did consulting at Tower Semiconductor. I designed PCI communication circuits for IPC between a Graphics Processor Unit (GPU) and memory while consulting for Rendition, Inc. From 1994 to 1996, I worked on the design of displays at MTI. This work was at a time when cathode ray tubes (CRTs) were still the dominant type of display. Flat panel displays were being

developed with the hope of replacing CRTs in the consumer market. I worked on flat panel displays which resulted in five patents: U.S. Patent Nos. 5,598,156, 5,638,085, 5,818,365, 5,894,293, and 5,909,201. I worked on the design of the pixels, both active and passive, as well as the supporting electronics for processing video signals. I was involved with the evaluation of display technologies including liquid crystal displays (LCDs), light-emitting diodes, plasma displays, and organic light emitting diode (OLED) displays; the display technologies that were looking to displace CRTs in the consumer market. I was also involved with the packaging of the displays including the vacuum sealing and deposition of the phosphors for light wavelength conversion. I also taught display design as a topic in my courses and did display design consulting again in industry for Cirque in 2013.

12. My current research work is focused in part on the design of integrated circuits for wireless sensing using LIDAR (Light Detection And Ranging). I have worked with several companies in the development of these circuits and systems including Freedom Photonics, Aerius Photonics, and FLIR. In the early 1990s, I worked on wireless systems for wideband impulse radar while at Lawrence Livermore Laboratory. Further, part of my research for several years focused on the digitization of IQ channels using delta-sigma modulation. The knowledge and experience gained from this effort are reflected in my textbook CMOS Mixed-Signal

Circuit Design and a presentation, which I have presented at several universities and companies, http://cmosedu.com/jbaker/papers/talks/BP_DSM_talk.pdf.

c. Academic Experience

13. I was an adjunct faculty member in the Electrical Engineering departments of UNLV and UNR from 1991-1993. From 1993 to 2000, I served on the faculty at the University of Idaho as an Assistant Professor and then as a tenured Associate Professor of Electrical Engineering. In 2000, I joined a new Electrical and Computer Engineering program at Boise State University (“BSU”), where I served as department chair from 2004 to 2007. At BSU, I helped establish graduate programs in Electrical and Computer Engineering including, in 2006, the university’s second Ph.D. degree. In 2012, I re-joined the faculty at UNLV. Over the course of my career as a professor, I have advised more than 100 masters and doctoral students.

14. I have been recognized for my contributions as an educator in the field. While at BSU, I received the President’s Research and Scholarship Award (2005), Honored Faculty Member recognition (2003), and Outstanding Department of Electrical Engineering Faculty recognition (2001). In 2007, I received the Frederick Emmons Terman Award (the “Father of Silicon Valley”). The Terman Award is bestowed annually upon an outstanding young electrical/computer engineering educator in recognition of the educator’s contributions to the profession. In 2011, I

received the IEEE Circuits and Systems Education Award. I received the Tau Beta Pi Outstanding Electrical and Computer Engineering Professor Award every year it was awarded while I have been back at UNLV.

15. I have authored several books and papers in the electrical and computer engineering area. My published books include CMOS Circuit Design, Layout, and Simulation (Baker, R.J., Wiley-IEEE, ISBN: 9781119481515 (4th ed., 2019)) and CMOS Mixed-Signal Circuit Design (Baker, R.J., Wiley-IEEE, ISBN: 9780470290262 (2nd ed., 2009) and ISBN: 9780471227540 (1st ed., 2002)). I co-authored DRAM Circuit Design: Fundamental and High-Speed Topics (Keeth, B., Baker, R.J., Johnson, B., and Lin, F., Wiley-IEEE, ISBN: 9780470184752 (2008)), DRAM Circuit Design: A Tutorial (Keeth, B. and Baker, R.J., Wiley-IEEE, ISBN: 0-7803-6014-1 (2001)), and CMOS Circuit Design, Layout and Simulation (Baker, R.J., Li, H.W., and Boyce, D.E., Wiley - IEEE, ISBN: 9780780334168 (1998)). I contributed as an editor and co-author on several other electrical and computer engineering books.

d. Other Relevant Experience

16. I have performed technical and expert witness consulting for more than 200 companies and their subsidiaries and given more than 50 invited talks at conferences, companies, and universities. Further, I am the author or co-author of

more than 100 papers and presentations in the areas of electrical and computer engineering design, fabrication, and packaging.

17. I currently serve, or have served, as a volunteer on the IEEE Press Editorial Board (1999-2004); as editor for the Wiley-IEEE Press Book Series on Microelectronic Systems (2010-2018); as the Technical Program Chair of the 2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS 2015); on the IEEE Solid-State Circuits Society (SSCS) Administrative Committee (2011-2016); as a Distinguished Lecturer for the SSCS (2012-2015); the Technology Editor (2012-2014) and Editor-in-Chief (2015-2020) for IEEE Solid-State Circuits Magazine; IEEE Kirchhoff Award Committee (2020-2023); and advisor for the student branch of the IEEE at UNLV (2013-present). These meetings, groups, and publications are intended to allow researchers to share and coordinate research. My active participation in these meetings, groups, and publications allowed me to see what other researchers in the field have been doing.

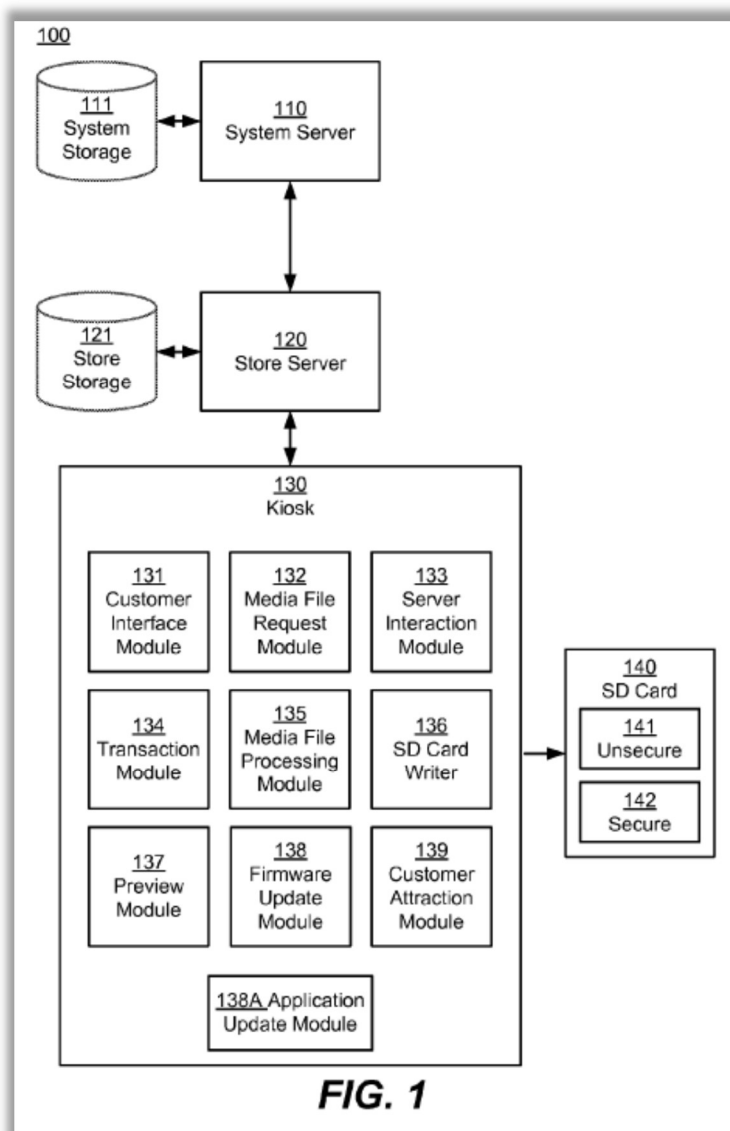
18. In addition to the above, I am an IEEE Fellow for contributions to semiconductor memory design and a member of the honor societies Eta Kappa Nu and Tau Beta Pi.

II. OVERVIEW OF THE '783 PATENT

19. As I understand it, the '783 Patent is directed to a kiosk for transferring content to a secure digital (SD) card, where the kiosk includes various modules for

customer interface, media file requests, server interaction, transaction processing, and SD card writing. The '783 Patent purports to describe improvements related to efficiently and securely writing encrypted content to an SD card.

20. After reviewing the '783 Patent specification and claims, it is my opinion that the patent describes a system for transferring digital media content to



an SD card through a kiosk-based distribution system, where the kiosk includes various functional modules for selecting, processing, and writing encrypted content

to both secure and unsecure areas of an SD card. These basic components are illustrated in Figure 1 of the patent, above.

21. The '783 Patent acknowledges that kiosk-based digital media distribution systems were already known in the prior art. For example, the patent states: "A method of distributing digital media content is through kiosk systems. . . The kiosk is connected via a network to one or more servers having access to storage of digital media content. Customers can interact with the kiosk, for example through a touch screen interface, to select desired digital media content for purchase." *See* Ex. 1001 at 1:20-26.

22. The '783 Patent also acknowledges that SD cards with secure and unsecure areas were previously known. For example, the patent states: "an SD card comprises a media device having computer readable and writable storage areas with a secure area and an unsecure area thereon." *See* Ex. 1001 at 2:8-12.

23. The '783 Patent describes using Content Protection for Recordable Media (CPRM) as a known standard for managing digital rights on secure media. *See* Ex. 1001 at 4:57-65.

24. Based on my experience in the field and my review of the '783 Patent, I believe that the essential elements claimed in the '783 Patent relate to a kiosk system incorporating various modules for facilitating the transfer of encrypted media

content to both secure and unsecure areas of an SD card, with a particular ordering of writing operations designed to optimize the writing process.

25. I have reviewed the prosecution history of the '783 Patent. The '783 Patent was filed on October 18, 2010, and claims priority to U.S. Provisional Application No. 61/253,789, which was filed on October 21, 2009. Ex. 1001 at 1:7-10. The earliest possible priority for the '783 Patent is therefore October 21, 2009. I have been asked to assume this earliest date as the priority date. All references asserted herein qualify as prior art to the '783 Patent.

III. LEGAL STANDARDS AND ASSUMPTIONS

26. I understand that there are several ways in which a patent claim may be shown to be unpatentable, including anticipation under 35 U.S.C. § 102 or obviousness under 35 U.S.C. § 103. In considering these issues, I have been informed that a person of ordinary skill in the art ("POSITA") is the hypothetical person who is presumed to have the relevant technical knowledge and familiarity with the relevant arts and state of the technology at the time of the alleged invention.

a. A Person of Ordinary Skill in the Art

27. Based on my knowledge and experience in the field of data storage and secure digital (SD) card technology, a POSITA relevant to the '783 Patent at the time of the alleged invention would have had a bachelor's degree in computer science, computer engineering, electrical engineering, or a related field, with two to

three years of experience in the field of data management. Alternatively, equivalent knowledge, experience, and skill could be obtained with a higher level of education and less professional experience, or through more years of professional experience with a lower level of education.

28. Given my education, background, and experience, it is my opinion that I exceed the level of a POSITA in the relevant field of the '783 Patent. I am therefore qualified to provide an opinion regarding what a POSITA would have known and understood at the time of the alleged invention.

b. Obviousness

29. I have been informed that a claimed invention is obvious, and thus unpatentable, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious to a POSITA at the time of the claimed invention.

30. I have also been informed that the determination of whether a claimed invention is obvious in view of the prior art cannot rely on hindsight, i.e., using the patent claim as a roadmap or template to select components from the prior art to reconstruct the claimed invention.

31. I have been informed that a POSITA is presumed to have been aware of all relevant prior art. I have also been informed that a POSITA is someone of ordinary creativity in the field who is presumed to have understood and considered

design needs and/or market forces which would have motivated or prompted them to seek variations of a product having utility in their field.

32. I have been informed that the determination of whether a claimed invention was obvious in view of the prior art is a legal question that involves an objective analysis of these factual factors:

- a. The scope and content of the prior art;
- b. The differences between the prior art and the claimed invention;
- c. The level of ordinary skill in the pertinent art; and
- d. Any secondary consideration(s) having a nexus to the claimed invention, for example: [i] its commercial success (or the lack thereof), [ii] whether the claimed invention satisfied a long felt but unmet need, [iii] unexpected results achieved by the claimed invention, or [iv] skepticism or failure by others.

33. I have also been informed that the above factors define an expansive and flexible framework to determine whether a claimed invention would have been obvious in view of the prior art.

34. When a prior art reference was available in one field, design incentives and other market forces could prompt variations of the reference by a POSITA either in the same field or a different field. If the POSITA could implement a predictable

variation that meets the elements of a patent claim, then the claimed invention was obvious.

35. Likewise, if a technique had been used to improve one device in the prior art, and a POSITA would recognize that the technique could also be used to improve similar devices in the same way, using that technique was obvious unless its actual application was beyond the capability of the POSITA.

36. The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. If an invention is no more than the predictable use of prior art elements according to their established functions, the combination was obvious unless its implementation was beyond the capability of the POSITA.

37. To determine whether there was an apparent reason to combine elements known in the prior art as claimed, it is often necessary to examine the interrelated teachings of multiple prior art references, the effects of demands known to the field or present in the market, and the background knowledge of a POSITA. This determination is not a rigid test. Rather, it must consider the inferences and creative steps that a POSITA would employ, because the POSITA is not an automaton.

38. Common sense teaches that familiar items may have obvious uses beyond their primary purposes, and in many cases a POSITA would have been able to fit the teachings of multiple patents together like pieces of a puzzle.

39. A motivation to combine the teachings of multiple prior art references may be suggested in one or more of the references, or found in the nature of the problem to be solved, in the trends or direction of the field and/or market, or come from the common sense and ordinary skill of the POSITA.

40. When there was a design need or market pressure to solve a problem and there were a finite number of identified, predictable solutions, a POSITA would have good reason to pursue the known options within his or her technical grasp. If this would have led to reasonably anticipated success, it was likely the product not of innovation but of ordinary skill and common sense, in which case the fact that a combination of known elements was obvious to try would show that the claimed invention was obvious.

IV. CLAIM CONSTRUCTION

41. I understand that, for purposes of this proceeding, terms in the claims of the '783 Patent are to be given their plain and ordinary meaning as would be understood by a POSITA at the time of the invention, in the context of the specification and prosecution history of the '783 Patent.

42. Based on this understanding and my review of the '783 Patent, I do not believe that any of the claim terms require explicit construction for purposes of my analysis in this declaration. However, I have discussed specific interpretations of certain claim elements as part of my analysis of the prior art below.

V. LEVEL OF ORDINARY SKILL IN THE ART

43. As stated above, in my opinion, a POSITA at the time of the alleged invention would have had a bachelor's degree in computer science, information systems, or a related field, with two to three years of experience in the field of data management. Alternatively, equivalent knowledge, experience, and skill could be obtained with a higher level of education and less professional experience, or through more years of professional experience with a lower level of education.

44. By October 2009, the earliest claimed priority date of the '783 Patent, there was substantial knowledge and experience in the field of digital media distribution kiosks, secure digital storage, and digital rights management. A POSITA would have been familiar with SD card technology, encryption technologies related to secure media content distribution, and software interfaces for media content selection and transfer.

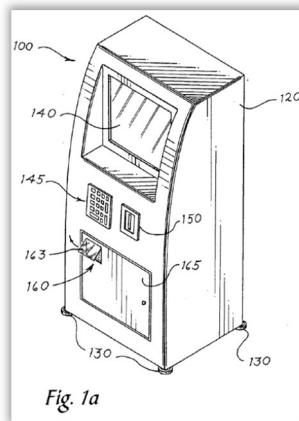
VI. PRIOR ART REFERENCES

45. In forming my opinions, I have considered the following prior art references, among others:

**a. U.S. Patent Publication No. 2009/0113116 (“Thompson”)
(Ex. 1005)**

46. Thompson discloses a digital content kiosk for writing digital media onto removable solid-state memory devices. Thompson was filed on October 30, 2007, and published on April 30, 2009, more than one year before the filing date of the '783 Patent, and is therefore prior art under 35 U.S.C. § 102(e) (pre-AIA).

47. Thompson discloses a kiosk-based digital media distribution system.



(FIG. 1A of Thompson Ex. 1005)

48. Thompson’s kiosk-based system provides a means for a user to select and pay for media from a kiosk for download onto an external memory device. The media is encrypted and can later be decrypted by a key stored in a restricted area of the user’s memory device. Specifically, Thompson’s kiosk system:

receives a selection of video content either manually from a user using
the touch-screen display 140 and/or the key pad 145.

Ex. 1005 at [0044].

[t]he control program and electronics 2300 can then present a payment screen to facilitate the purchase of the video content and removable memory device.

Id. at [0017]

Video content is encrypted and decrypted using a secure key (CEK) contained within the memory device and not accessible outside of it.

Id. at [0111].

49. Thompson specifically discloses that the kiosk can interface with various types of media, and explicitly mentions that the “kiosk can be altered to use other types of devices,” and “can use any type of media.” *See* Ex. 1005 at [0033], [0037]. A POSITA would understand that this would include SD cards, which were common removable storage media at the time. *See* Ex. 1001 at 2:8-12.

50. Thompson discloses writing encrypted content to an unsecure area of a memory device and separately storing encryption keys in a secure area of the memory device. *See* Ex. 1005 at [0105]-[0106]; *id.* at Fig. 22 a:

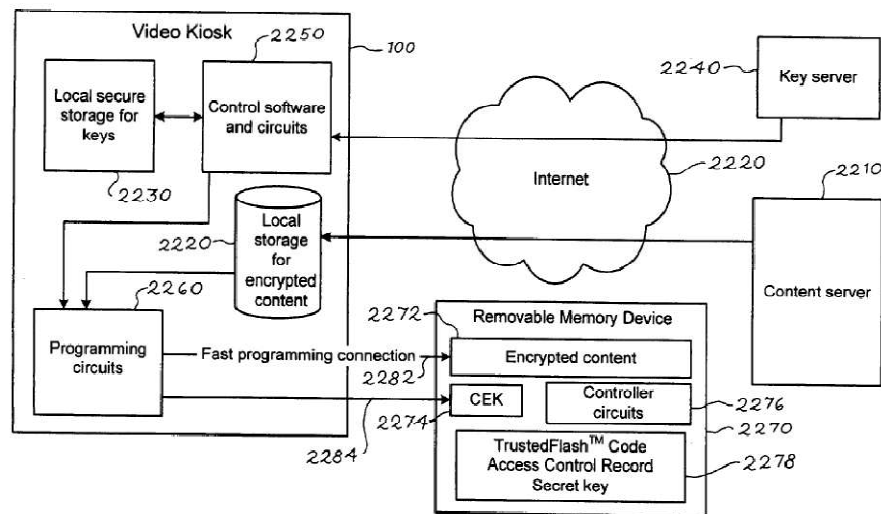


Fig. 22 a

51. Thompson also notes that writing to the secure area is slower than writing to the unsecure area, stating: “Since the CEK [Content Encryption Key] comprises only a relatively limited amount of data, the delay caused by using a secure transfer mechanism should not be that noticeable to the user.” *See* Ex. 1005 at [0106].

b. U.S. Patent Publication No. 2007/0116268 (“Kasahara”) (Ex. 1007)

52. Kasahara discloses a system for secure delivery of digital content data to SD cards. Kasahara was published on May 24, 2007, more than one year before the filing date of the ’783 Patent, and is therefore prior art under 35 U.S.C. § 102(b).

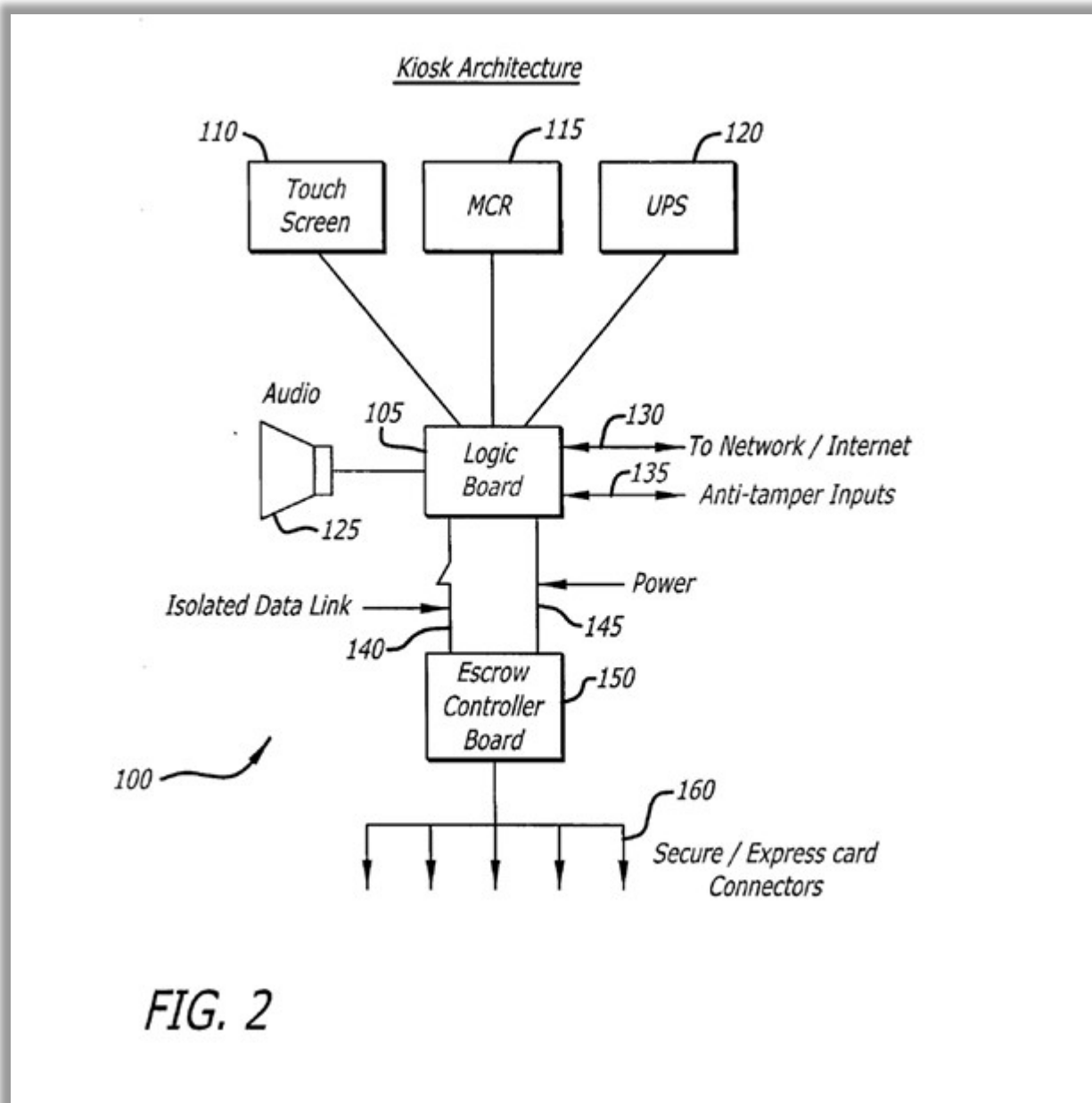
53. Kasahara specifically describes a system for delivering encrypted content to SD cards, in which encrypted media content is stored in an SD card’s unsecure area, and encryption keys, including a content key and user key, are stored in the same SD card’s secure area. Ex. 1007 at Abstract, [0044], and [0046].

54. Kasahara discloses that the encryption keys are stored in the secure portion of an SD card, and that the content key is encrypted with a user key: “The SDSD content key data Kcib is encrypted with the SDSD user key data Kub to be an Enc (Kub:Kcib) and then also stored in the user area of the SD card 20. The SDSD user key data Kub itself is stored in the protection area of the SDSD card 20 in such a way that the SDSD user key data Kub may be inaccessible from outside.” See Ex. 1007 at [0061].

c. U.S. Patent Publication No. 2010/0205023 (“Wagner”) (Ex. 1006)

55. Wagner discloses a system for high-speed digital media distribution, focusing on optimizing data transfers to secure and portable storage devices. Wagner was filed on February 2, 2010, and published on August 12, 2010, which makes it prior art under 35 U.S.C. § 102(e).

56. Wagner discloses a kiosk-based content delivery system where media content is encrypted and protected using digital rights management. Ex. 1006 at Abstract; *see also id.* at Fig. 2:



57. Wagner discloses that the media content purchased or rented from the kiosk could be encrypted with appropriate digital rights management information. *Id.* at [0043].

58. Wagner explains that for a user to access the encrypted media content, the user would need to have an encryption key:

When the user desires to play the encrypted data content back, the user would need to have the right to access the encrypted content, **access which would be granted by providing the key once the purchase or rental transaction had taken place.** Of course, there are many digital rights management systems currently available for use, and the various embodiments of the systems of the present invention are capable of being adapted or upgraded to allow their use. This ability to upgrade the systems is also useful in that the systems may be upgraded to use future digital rights management systems developed in the future. Moreover, since content owners may select differing digital rights management systems for their content, the system will also be able to simultaneously support different digital rights management systems so that the wider choice of content can be made available to a consumer for purchase or rent.

Id. at [0055] (emphasis added).

59. Wagner specifically discloses that the system can be used to encrypt the content in an exceptionally secure manner because the encryption key can be tied to the secure flashcard itself. Ex. 1006 at [0062].

d. Enabling Secure Distribution of Digital Media to SD Cards (“Ponceleon”) (Ex. 1008)

60. Ponceleon is a publication discussing high-speed secure digital media distribution to SD cards. It was published in October 2006, more than one year

before the filing date of the '783 Patent, and is therefore prior art under 35 U.S.C. § 102(b). Ex. 1012 Declaration of Sylvia D. Hall-Ellis, PH.D. (“Hall-Ellis Decl.”) at ¶ 58.

61. Ponceleon discloses high-speed, kiosk-based downloading of media content and CPRM (Content Protection for Recordable Media) enforcement through the use of SD cards.

62. As Ponceleon discloses, “CPRM is based on broadcast encryption, and it is a standard feature of SD memory cards. Ex. 1008 at 495.

63. Ponceleon’s system discloses a kiosk which accepts an SD card from a user. *Id.* at 496. Thereafter, the kiosk “presents the user with a list of the titles available for rental or purchase. User selects a title and pays for the title.” *Id.* Ponceleon discloses that thereafter, “kiosk starts recording the encrypted content to the SD card,” and the “licensing server” “verifies payment and generates a title binding token.” *Id.* This token “contains the decryption key necessary for content playback,” and the kiosk “writes [the token] to the protected area of the SD card.” *Id.* This system is shown in Figure 1:

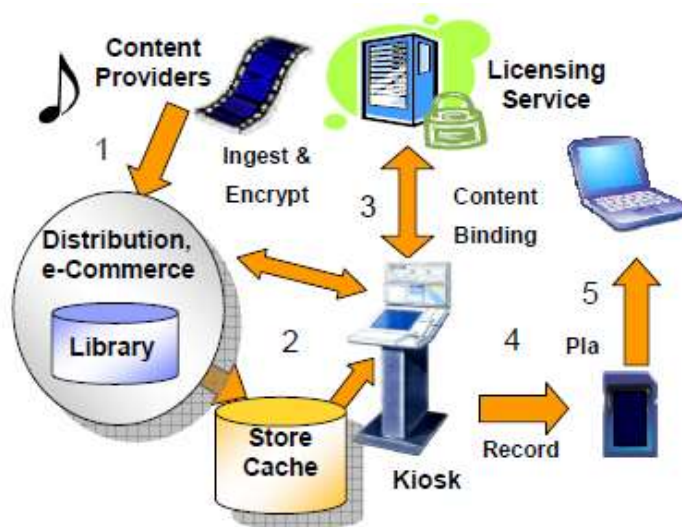
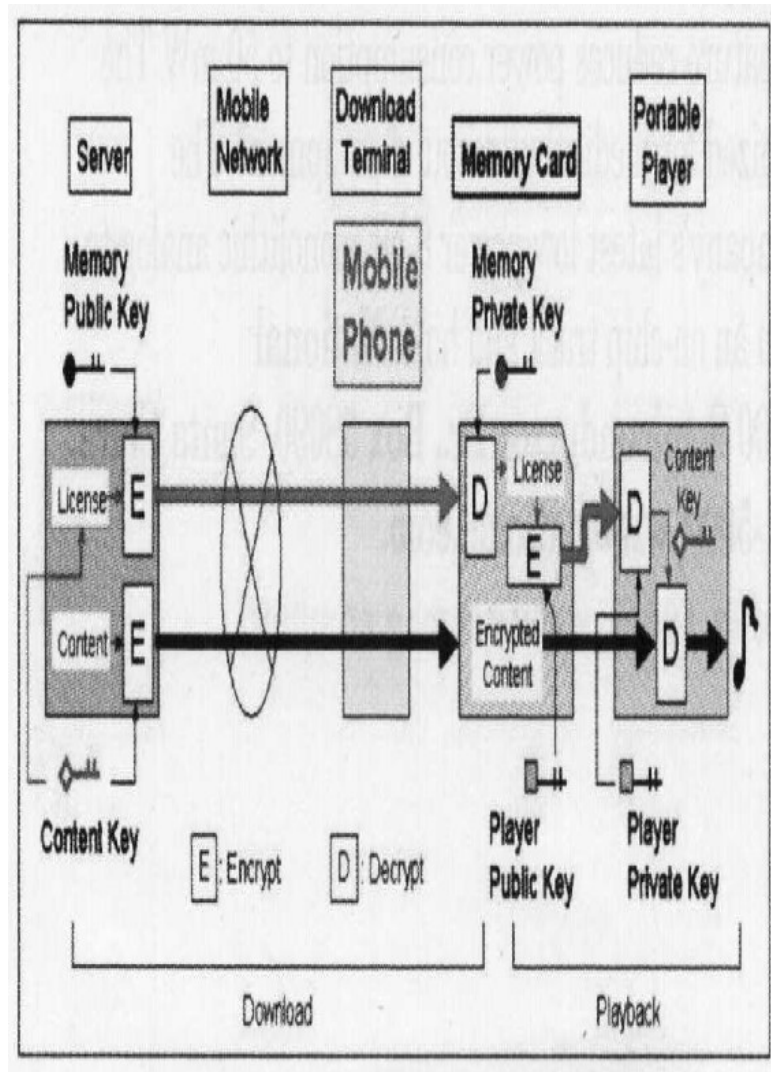


Figure 1: Secure Multimedia Distribution Architecture

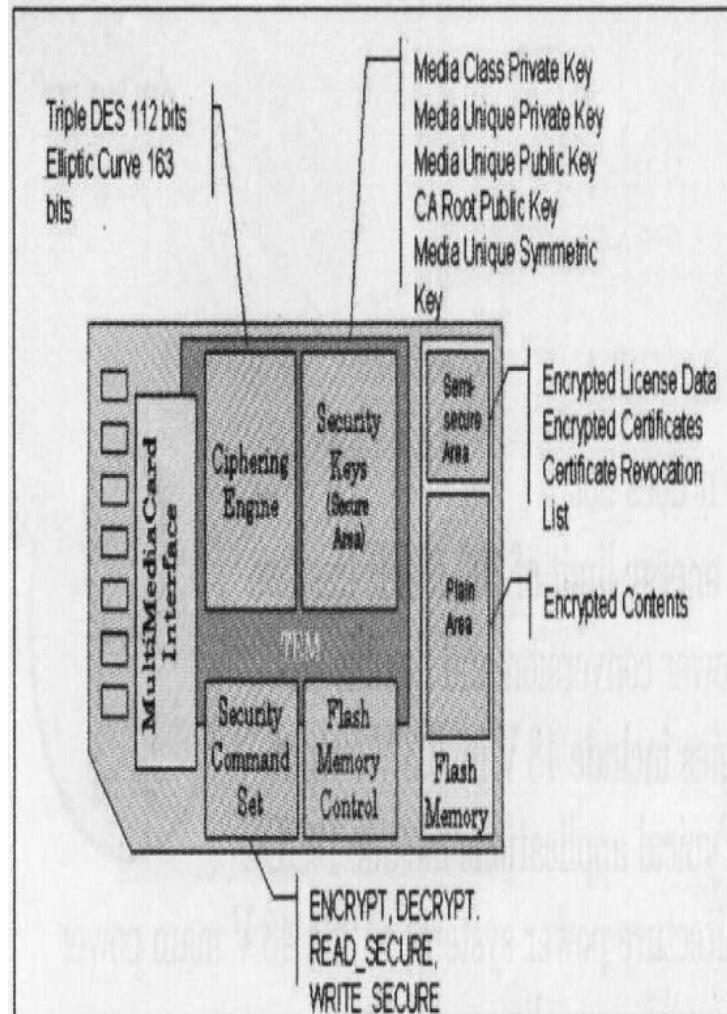
**e. Secure MultiMediaCard for Content Protection (“Ishihara”)
(Ex. 1009)**

64. Ishihara is a publication describing secure content protection systems for multimedia cards. It was published on December 15, 2001, more than one year before the filing date of the '783 Patent, and is therefore prior art under 35 U.S.C. § 102(b). Ex. 1012, ¶ 58.

65. Ishihara discloses a content protection system where encryption keys are pre-configured in the secure area of a memory card. This provides a framework where encrypted content is stored on the card, and access is controlled through licensing systems. This system is shown in the figure below:



66. Ishihara further discloses a Public Key Infrastructure (PKI)-based approach to digital rights management. Ex. 1009 at p. 23, 26. The system ensures that encrypted media remains secure by storing decryption keys in a tamper-resistant module, preventing unauthorized access. Ex. 1009 at p. 23, 26. An example of this type of secure storage device is depicted in the figure below:



VII. GROUND 1: CLAIMS 1-3, 5-8, 10-13, 15, and 16 ARE OBVIOUS UNDER §103 OVER THOMPSON IN VIEW OF KASAHARA

67. Thompson and Kasahara, alone or in combination, teach each and every limitation of Claims 1-3, 5-8, 10-13, 15, and 16 and therefore render these claims obvious.

a. Motivation to Combine Thompson and Kasahara

68. In my opinion, a POSITA would have been motivated to combine the teachings of Thompson and Kasahara for several reasons. Both references address the same fundamental problem of securely distributing digital media content to portable storage devices, and both disclose systems for encrypting and protecting digital content.

69. Thompson describes a kiosk system for transferring digital content to portable storage media (Ex. 1005 at [0032]), while Kasahara provides specific details on implementing encryption and secure content management for SD cards (Ex. 1007 at [0009]). A POSITA would have recognized that combining these complementary technologies would result in an improved system with enhanced security and efficiency.

70. Both references are in the same field of endeavor (secure content delivery to memory devices) and both solve similar problems related to content security. A POSITA would have found it natural to look to Kasahara's specific SD card encryption techniques to enhance Thompson's more general kiosk-based media distribution platform.

71. Thompson discloses that its system can be adapted to various types of memory devices, stating that the "kiosk can be altered to use other types of devices," which can be "any type of media" (Ex. 1005 at [0033], [0037]). A POSITA would

have understood this to include SD cards, which were common portable storage media at the time of the invention. *See, e.g.*, Ex. 1001 at 2:8-12.

72. Kasahara's encryption system, which uses a user key to encrypt a content key that in turn encrypts the content data (Ex. 1007 at [0061]), would have been recognized by a POSITA as a robust solution for securing digital content in Thompson's kiosk environment. This tiered encryption approach was well-known in the field for providing strong content protection while still allowing authorized access.

73. Given the increasing need for secure and efficient media transactions in the digital marketplace, a POSITA would have been motivated to combine these references to enhance both security and reliability in digital content distribution systems. The combination would require only routine modifications using well-known techniques to achieve predictable results.

b. Claim 1 Analysis

i. 1[pre]: A kiosk for transferring content to a secure digital (SD) card, the kiosk comprising:

74. To the extent that the preamble is limiting, Thompson and Kasahara, either alone or in combination, teach this subject matter.

75. Thompson discloses "a digital content kiosk for on-the-fly programming of digital content onto a removable solid-state memory device" (Ex. 1005 at [0031], Figs. 1a-1b, 22a). While Thompson does not explicitly identify the

removable memory device as an “SD card,” Thompson defines a “removable solid-state memory device” as “a memory device that uses a solid-state memory array to store data” (Ex. 1005 at [0036]). A POSITA would have understood this definition to include SD cards, which were common solid-state memory devices at the time. *See* Ex. 1001 at 2:8-12.

76. Moreover, Thompson explicitly states that a “kiosk can be altered to use other types of devices,” which can be “any type of media” (Ex. 1005 at [0033], [0037]). Given that SD cards were well-known and widely used memory devices at the time, it would have been obvious to a POSITA to modify Thompson’s kiosk to use an SD card as the output medium.

77. Additionally, Kasahara explicitly discloses a content delivery system for delivering content to an SD card (Ex. 1007 at [0032]-[0033]). Kasahara describes a system where “a user may have a personal computer (PC) 10, a SD memory card (SD card) 20, and a handheld terminal 30 (user terminal)” and “[t]he user connects the SD card 20 to the PC 10 to access the server 50, and downloads. . . encrypted content data” (Ex. 1007 at [0032]-[0033]). Kasahara also mentions that this content delivery system can be used in “stores, such as a convenience store, [where] a store terminal 40 that is [] connected via the Internet or a leased (dedicated) line to the server [that provides the content]” (Ex. 1007 at [0033]).

78. Based on these disclosures, it would have been obvious to a POSITA to adapt Kasahara's content delivery system to a physical store terminal such as the kiosk disclosed by Thompson.

ii. 1[a]: a customer interface module for receiving a customer's selection of a plurality of media files to transfer to the SD card;

79. Thompson teaches this claim limitation. Thompson discloses a video kiosk 100 that "receives a selection of video content either manually from a user using the touch-screen display 140 and/or the key pad 145" (Ex. 1005 at [0044]). The touch-screen display 140 and the key pad 145 constitute a "customer interface module" because they present a user interface through which a customer can select media to download to a memory device (Ex. 1005 at [0038], [0044]).

80. The '783 Patent describes the "customer interface module" as one that "manages a graphical user interface presented to a customer, through which, the customer can select media to preview at the kiosk 130 or download to the customer's SD card" (Ex. 1001 at 4:5-8). Thompson's touch-screen display 140 and key pad 145 perform the same function, allowing a user to select media for download.

81. As discussed for the preamble, Thompson's kiosk system could be modified to use an SD card as an output medium, as Thompson explicitly states that a "kiosk can be altered to use other types of devices," which can be "any type of media" (Ex. 1005 at [0033], [0037]).

iii. 1[b]: a media file request module for requesting the plurality of media files and corresponding metadata file for each media file from a server communicatively coupled to the kiosk;

82. Thompson teaches this claim limitation. Thompson discloses a system that requests media files based on a user's selection. Specifically, Thompson states that "the video kiosk 100 can connect to an external network location to retrieve video content on-the-fly when requested by a user or to retrieve video content for local storage on one or more mass storage devices in the video kiosk 100" (Ex. 1005 at [0042]). Thompson further explains that "after video content is selected, the control program and electronics 2300 can display another screen presenting options for the quality level of the video content versus price, which can be updated based on the available media in the video kiosk 100," (Ex. 1005 at [0117]) and "the control program and electronics 2300 can retrieve the selected video content from the video content server." (Ex. 1005 at [0118]).

83. The '783 Patent describes the "media file request module" as one that "receives the user's selections of media from the customer interface module 131 and prepares a request for the corresponding media files, for example, by performing a lookup of the selected media file" (Ex. 1001 at 4:16-21). A POSITA would have understood that Thompson's "control program" performs the functionality of "a media file request module" by receiving a request for a media file from a user and

looking up the availability of said file, both on the kiosk's local storage, and on the video content server.

84. While Thompson does not explicitly mention "metadata files," it would have been obvious to a POSITA that a download of a video file would typically include metadata. The '783 Patent explains that "[m]etadata includes the title of the playable content, and expanded descriptive information about the content, such as the actors, the director, and/or other information that may appear on or inside a DVD box, for example" (Ex. 1001 at 3:36-39).

85. Thompson discloses that the control program and electronics 2300 can load "extra features" or "additional video" (Ex. 1005 at [0123]). Including metadata such as title information and descriptive content with the download of a video file would have been obvious to a POSITA, as such information is useful to display to the user during playback of the video content and was common practice in video rental systems at the time.

iv. 1[c]: a server interaction module for receiving the requested plurality of media files and the corresponding metadata files from the server;

86. Thompson teaches this claim limitation. Thompson discloses a kiosk that receives media files from a server. Specifically, Thompson states that "if the local mass storage device 2200 does not have a video title desired by a user, the video kiosk 100 can contact the content server 2210 on-the-fly to download the

desired video content” (Ex. 1005 at [0101]). Thompson further explains that “the control program and electronics 2300 can retrieve the selected video content from the video content server.” (Ex. 1005 at [0118]).

87. The ’783 Patent describes the “server interaction module” as one that “manages communications between the kiosk 130 and the store server 120” and “receives media files from the store server 120 that are distributed to the kiosk 130” (Ex. 1001 at 4:22-29). A POSITA would have understood that Thompson’s “control program” performs the functionality of “a server interaction module” by receiving video content from an external network location based on user requests.

88. As discussed for limitation 1[b], while Thompson does not explicitly mention “metadata files,” it would have been obvious to a POSITA that a download of a video file would typically include associated metadata such as title information, descriptions, and other content-related information.

v. 1[d]: a transaction module for accepting payment from a customer for the customer’s selection of the plurality of media files to transfer to the SD card;

89. Thompson teaches this claim limitation. Thompson discloses a payment input device which allows a user to purchase video content from the video kiosk (Ex. 1005 at [0040]). Thompson specifically states that “[t]he control program and electronics 2300 can then present a payment screen to facilitate the purchase of the video content and removable memory device” (Ex. 1005 at [0117]).

90. The '783 Patent describes the “transaction module” as one that “manages the payment detail of the customer’s purchase from the kiosk 130. The transaction module 134 receives the customer’s payment information, for example from information read from the swipe of a card through a card reader...” (Ex. 1001 at 4:30-34).

91. A POSITA would have understood that Thompson’s “control program” is used to “accept payment from a customer,” as Thompson explains that the “control program and electronics 2300 can then present a payment screen to facilitate the purchase of the video content,” thus performing the same functions as the “transaction module” claimed in the ‘783 Patent (Ex. 1005 at [0117]).

vi. 1[e]: an SD card writer for writing data to an unsecure user area of the SD card and a protected secure area of the SD card; and

92. Thompson and Kasahara, either alone or in combination, teach this claim limitation. Thompson discloses programming circuits to program encrypted video content and associated keys into a solid-state memory device (Ex. 1005 at [0105]). Thompson explains that, “[a]s the data is transferred to the device, it is encrypted by the encryption engine and stored in an encrypted format in a restricted region of the memory device” (Ex. 1005 at [0112]). Thompson further states that the content “is encrypted and decrypted using a secure key (CEK) contained within the memory device and not accessible outside of it” (Ex. 1005 at [0111]).

93. Thompson's memory device also contains a user area that is not secured for storing certain data including, for example, "content identification" information "assigned by the kiosk when loading the content" that is subsequently used for user authentication (Ex. 1005 at [0113]).

94. A POSITA would have understood that Thompson's "programming circuits" function as a writer for writing data into both an unsecure user area and a protected secure area of a memory device.

95. As discussed for the preamble, Thompson's system could be modified to use an SD card as the output medium, as Thompson explicitly states that a "kiosk can be altered to use other types of devices," which can be "any type of media" (Ex. 1005 at [0033], [0037]).

96. Additionally, Kasahara explicitly differentiates between writing to secure and unsecure areas of an SD card. Kasahara's SD card 20 includes a user area and a protection area (Ex. 1007 at [0061]). Kasahara discloses writing content in the user area of the SD card and key data in the protected area of the SD card 20: "The handheld terminal 30 stores the encrypted content data Enc (Kcib:Ci) in the user area of the SD card 20. The SDSD content key data Kcib is encrypted with the SDSD user key data Kub to be an Enc (Kub:Kcib) and then also stored in the user area of the SD card 20. The SDSD user key data Kub itself is stored in the protection

area of the SDDS card 20 in such a way that the SDDS user key data Kub may be inaccessible from outside” (Ex. 1007 at [0061]).

97. A POSITA would have understood that Kasahara’s system includes an SD card writer for writing data into both an unsecure user area and a protected secure area of an SD card.

vii. 1[f]: a media file processing module for preparing the plurality of media files and the corresponding metadata files to be written to the SD card in cooperation with the SD card writer,

98. Thompson and Kasahara, either alone or in combination, teach this claim limitation. Thompson’s kiosk comprises control program and electronics 2300 which constitutes a media file processing module. Like the “media file processing module” disclosed by the ’783 Patent, Thompson’s control program and electronics “retrieve[s] the selected video content from the video content servers”, and “initiate[s] the media programming process” (Ex. 1005 at [0117]-[0118]).

99. The ’783 Patent describes the “media file processing module” as one that “processes media files in preparation for writing the files to SD cards 140. The media file processing module 135 receives the requested media files from the store server 120 via the server interaction module 133. The media file processing module 135 then queues the media file for download to the SD card 140” (Ex. 1001 at 4:42-47).

100. A POSITA would have understood that Thompson's control program provides the same functionality as the '783 Patent's "media file processing module."

101. Kasahara likewise discloses a system of controlled content retrieval, encryption, and storage, which involves the process of "download[ing] from a content-data download site provided by the server 50 content data" (Ex. 1007 at [0033]). A POSITA would have understood that Kasahara's system provides the same functionality as the '783 Patent's "media file processing module."

viii. 1[g]: wherein space is pre-allocated on the SD card for writing an encrypted playable content portion of each media file to an unsecure area of the SD card, and

102. Thompson and Kasahara, either alone or in combination, teach this claim limitation. The control program and electronics 2300 of Thompson optimizes the use of available memory space when programming the media content onto the memory device. Thompson states that "[t]he control program and electronics 2300 can also contain sales delivery optimization algorithms to calculate available space on a to-be- (or already-) programmed memory device and can provide flexible on-the-fly-delivery of video content based on that calculation" (Ex. 1005 at [0120]). Thompson's system also analyzes available space before writing: "The control program and electronics 2300 can also determine that programming a memory device with the selected video content will result in unused space in the memory device" (Ex. 1005 at [0121]).

103. A POSITA reading Thompson would find pre-allocating space on the memory device for encrypted playable content to be inherently taught in Thompson or obvious, because Thompson's optimization and memory scanning functionality would necessarily allocate the optimal space for the encrypted content that was to be programmed. Even if not explicitly stated, pre-allocation would be an obvious design choice, as the system would need to ensure sufficient space was available before beginning the writing operation.

104. Further, Thompson discloses writing an encrypted playable content portion of each media file to an unsecure portion of a memory device: "as shown in FIG. 22a, it is preferred that the encrypted video content 2272 be programmed in the removable memory device 2200 using a fast programming connection because of the relatively-large file size of the encrypted video content 2272" (Ex. 1005 at [0105]). A POSITA would have understood that this "encrypted video content" is stored in the "unsecure area" of the memory device, as the secure area is reserved for the encrypted key (Ex. 1005 at [0106]): "The programming circuits 2260 also program the associated content encryption key ('CEK')".

105. Additionally, as discussed above, Kasahara expressly distinguishes between a user area ("unsecure area") and a protection area of the SD card. Kasahara discloses that, while the "SDSD content key data Kub" used to encrypt the content

is stored in the protection area (“secure area”), the encrypted content is stored in the user area (“unsecure area”) (Ex. 1007 at [0061]).

106. The benefits of storing video content data to the unsecure portion of an SD card, while storing relatively small-file size data, such as keys, to the secure portion of an SD card, would have been obvious to a POSITA combining the teachings of Thompson and Kasahara.

ix. 1[h]: wherein, except for a user key, data to be written to the unsecure area of the SD card is queued for writing in advance of data to be written to a secure area of the SD card, such that the data to be written to the unsecure area is written in time before the data to be written to the secure area is written, and

107. Thompson and Kasahara, either alone or in combination, teach this claim limitation. The '783 Patent explains that the benefit of writing media content to an unsecure area of the SD card before writing data to a secure area of the SD card was to avoid “delay” as writing to a secure portion of the SD card is slower than writing to the unsecured portion (Ex. 1001 at 9:57-64).

108. Thompson discloses writing content data to an unsecure portion of a memory device (Ex. 1005 at [0105]) and encrypted content keys to a secure portion of a memory device (Ex. 1005 at [0106]). Furthermore, Thompson acknowledges that writing to the secure portion of the memory device could cause delays: “Since the CEK 2272 comprises only a relatively limited amount of data, the delay caused

by using a secure transfer mechanism should not be that noticeable to the user” (Ex. 1005 at [0106]).

109. Given Thompson’s recognition that writing to the secure portion causes delay, it would have been obvious to a POSITA to write media content to the unsecure area of the memory device before writing data to the secure area to minimize the impact of this delay on the overall writing process. A POSITA would have been motivated to queue the larger media files for writing to the unsecure area first, then complete the process by writing the smaller key data to the secure area.

110. Additionally, Kasahara discloses the process of storing encrypted content data in the user area (“unsecure area”) of the SD card 20 before key data is written to the secure area (Ex. 1007 at [0033]). As Kasahara explains, after downloading this content to an unsecure area, “[a]t this point, the user does not have the content key data Kcis” (Ex. 1007 at [0033]). Only later does Kasahara disclose saving content key data in the secure area of the SD card (Ex. 1007 at [0061]: “The SDSD content key data Kcib is encrypted with the SDSD user key data Kub and then also stored in the user area of the SD card 20”). Then the SDSD user key data Kub is stored in the protection area (“secure area”) of the SD card 20.

x. 1[i]: wherein the playable media files are encrypted by a content key that is encrypted by the user key.

111. Thompson and Kasahara, either alone or in combination, teach this claim limitation. The ’783 Patent explains that “[t]he user key is encrypted with the

SD cards ‘media key’ in an operation which can only be performed on the SD card through special interactions with the SD card’s secured area” (Ex. 1001 at 7:50-53).

112. Thompson discloses that “video content is encrypted using a secure key (CEK) contained within the memory device and not accessible outside of it” (Ex. 1005 at [0111]).

113. Kasahara more explicitly discloses the claimed hierarchical encryption structure, stating that the content key data is encrypted with user key data: “The SDSD content key data Kcib is encrypted with the SDSD user key data Kub and then also stored in the user area of the SD card 20” (Ex. 1007 at [0061]). Kasahara further discloses that the content data itself (i.e., the “playable media files”) are “encrypted with the content key data” (Ex. 1007 at [0009]).

114. It would have been obvious to a POSITA to combine Kasahara’s encryption method (using a user key to encrypt a content key which encrypts content data) with the system disclosed by Thompson. This encryption approach was a well-known technique for securing digital content while still allowing authorized access.

115. Based on my analysis of each limitation of Claim 1, it is my opinion that the combination of Thompson and Kasahara renders Claim 1 obvious to a POSITA at the time of the alleged invention.

c. Claim 2 Analysis

i. 2[pre]: The kiosk of claim 1,

116. As explained above, Thompson and Kasahara, alone or in combination, render obvious Claim 1.

ii. 2[a]: further comprising a preview module for playing a preview of content of selected [sic] by the customer through the kiosk while the SD card writer writes the plurality of media files to the SD card, wherein the preview of content selected by the customer includes content from the plurality of media files being written to the SD card.

117. Thompson teaches this claim limitation. Thompson discloses a “control program and electronics” that “display movie trailers or advertisements on the video touch screen. . .” (Ex. 1005 at [0115]). Thompson further states that these previews can be viewed while the SD card writer writes the plurality of media files to the SD card: “As the memory device is being programmed, the control program and electronics 2300 can display trailers of related video titles, advertisements, options to search and purchase other video content, and options to provide other services” (Ex. 1005 at [0117]).

118. The ’783 Patent describes the “preview module” as one that “manages the playback of preview of media files that are available for purchase. The preview module 137 can operate in parallel with the SD card writer” (Ex. 1001 at 5:1-6).

119. A POSITA would have understood that Thompson’s control program performs the same functions as the “preview module” claimed in the ’783 Patent, allowing users to view previews while content is being written to the memory device.

120. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara renders Claim 2 obvious to a POSITA at the time of the alleged invention.

d. Claim 3 Analysis

i. 3[pre]: The kiosk of claim 1,

121. As explained above, Thompson and Kasahara, alone or in combination, render obvious Claim 1.

ii. 3[a]: further comprising a firmware update module for transferring a firmware update to the SD card.

122. Thompson teaches this claim limitation. Thompson discloses a video kiosk that can update firmware of a memory device: “when the video kiosk 100 contacts the memory device 2600”, firmware stored in the “memory array” 2610 (contained within the Memory Device) “can be updated” (Ex. 1005 at [0130] – [131]).

123. The ’783 Patent explains that “[t]he firmware update module 138 receives firmware updates (e.g., firmware software updates). . . for use in updating firmware on the playback devices that use the SD cards 140” (Ex. 1001 at 5:17-21).

124. A POSITA would have understood that Thompson's kiosk, which provides the functionality of downloading firmware updates onto a flash card, necessarily included the type of "firmware update module" claimed in the '783 Patent.

125. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara renders Claim 3 obvious to a POSITA at the time of the alleged invention.

e. Claim 5 Analysis

i. 5[pre]: The kiosk of claim 1,

126. As explained above, Thompson and Kasahara, alone or in combination, render obvious Claim 1.

ii. 5[a]: further comprising a customer attraction module for playing segments from media files currently available for download from the kiosk while the kiosk is not used for purchase of a media file.

127. Thompson teaches this claim limitation. Thompson's kiosk comprises control program and electronics 2300, storage devices 2310 and a video touch screen 140 (Ex. 1005 at [0114]). Thompson discloses that the control program and electronics "display movie trailers or advertisements on the video touchscreen 140 while waiting for an active user" (Ex. 1005 at [0115]). The trailers or advertisements are "stored in the storage device 2310" of the kiosk (Ex. 1005 at [0115]).

128. The '783 Patent explains that “The customer attraction module 139 plays preview, such as movie previews, short segments of media files, and/or advertisements to download particular media files, in order to entice customers to make a purchase” (Ex. 1001 at 5:45-48).

129. A POSITA would have understood that Thompson’s control program and electronics 2300, storage devices 2310 and video touch screen 140 constitute a customer attraction module for playing media files available on the kiosk when the kiosk is not used for an active purchase.

130. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara renders Claim 5 obvious to a POSITA at the time of the alleged invention.

f. Claim 6 Analysis

i. 6[pre]: The kiosk of claim 1,

131. As explained above, Thompson and Kasahara, alone or in combination, render obvious Claim 1.

ii. 6[a]: further comprising a USB port to allow connection of the SD card with a USB adapter to the kiosk.

132. Thompson teaches this limitation. Thompson discloses that the kiosk “comprises a plurality of ports 180 to connect a PC-based control system of the video kiosk 100 to external ... peripherals” and the ports 180 specifically include “a USB port” (Ex. 1005 at [0042]).

133. At the time of the '783 Patent and Thompson's disclosure, USB-to-SD adapters were widely available and commonly used to allow electronic devices with USB ports to access SD cards. A POSITA would have recognized that a common use for a USB port is to interface with storage devices, including an SD card via a USB adapter.

134. Therefore, a POSITA would have found it obvious to use Thompson's disclosed USB port to connect an SD card (via a USB adapter) to the kiosk. This would have been a standard and obvious way to provide alternative connectivity options for different types of memory cards.

135. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara renders Claim 6 obvious to a POSITA at the time of the alleged invention.

g. Independent Claim 7 Analysis

i. 7[pre]: A method of quickly and securely transferring media files from a kiosk to a secure digital (SD) card, the method comprising:

136. For the same reasons explained for Claim 1[pre], Thompson and Kasahara, alone or in combination, teach a method of quickly and securely transferring media files from a kiosk to a secure digital (SD) card.

ii. 7[a]: identifying a media file for download to the SD card;

137. Thompson teaches this claim limitation. Thompson discloses requesting media files and corresponding metadata file from a server

communicatively coupled to the video kiosk: “the video kiosk 100 can connect to an external network location to retrieve video content on-the-fly when requested by a user or to retrieve video content for local storage on one or more mass storage devices in the video kiosk 100” (Ex. 1005 at [0042]); “if the local mass storage device 2200 does not have a video title desired by a user, the video kiosk 100 can contact the content server 2210 on-the-fly to download the desired video content. Preferably, the connection between the video kiosk 100 and the content server 2210 is suitably fast” (Ex. 1005 at [0101]).

138. A POSITA would have understood that Thompson discloses identifying a media file for download to the memory device (which could be an SD card as discussed for Claim 1[pre]).

iii. 7[b]: pre-allocating space on the SD card for a playable content portion of the media file, wherein the playable content portion of the media file is encrypted by a content key that is encrypted by a user key;

139. For the same reasons explained for Claim 1[g] and 1[i], Thompson and Kasahara, alone or in combination, teach pre-allocating space on the SD card for a playable content portion of the media file, wherein the playable content portion of the media file is encrypted by a content key that is encrypted by a user key.

iv. 7[c]: writing all directory blocks of the playable content portion of the media file together and, thereafter in time, writing all data blocks sequentially of the playable content portion of the media file; and

140. Thompson teaches this claim limitation. Thompson discloses pre-allocating space on the SD card for media file storage before writing, ensuring efficient content transfer: “The video kiosk 100 also comprises programming circuits 2260 to program encrypted video content and associated keys into a removable solid-state memory device 2270” (Ex. 1005 at [0105]).

141. Thompson also discloses that the data to be written may be divided into many portions, whereafter these portions are stored in sub-arrays, thus allowing for parallel writing of all information so stored (Ex. 1005 at [0072]).

142. Furthermore, it would have been obvious to a POSITA to write directory blocks of a media file prior to writing data blocks. Directory blocks store metadata such as file names, sizes, and locations of data blocks, while data blocks store the actual media content. Writing directory blocks first followed by sequential data blocks is a well-known technique in file system design, which ensures that the file system can properly reference the data before it is fully written. Modern file systems inherently use this approach for storage on removable media.

- v. **7[d]: writing all data that is to be written to an unsecure area of the SD card, including the encrypted playable content, prior in time to writing any data to a secure area of the SD card, except for the user key.**

143. For the same reasons explained for Claim 1[h], Thompson and Kasahara, alone or in combination, teach writing all data that is to be written to an unsecure area of the SD card, including the encrypted playable content, prior in time to writing any data to a secure area of the SD card, except for the user key.

144. Based on my analysis of each limitation of Claim 7, it is my opinion that the combination of Thompson and Kasahara renders Claim 7 obvious to a POSITA at the time of the alleged invention.

h. Claim 8 Analysis

- i. **8[pre]: The method of claim 7,**

145. As explained above, Thompson and Kasahara, alone or in combination, render obvious Claim 7.

- ii. **8[a]: wherein, except for a user key, data is only written to the secure area of the SD card if a transaction for the media file successfully completes.**

146. Thompson teaches this claim limitation. The '783 Patent explains that the purpose for writing data to the secure area of the SD card after transaction completion is to permit the user to decrypt and therefore view the downloaded media file: "if there is any kind of problem with the payment for the transaction through the transaction module 134 or with the transfer of the media file to the SD card 140, the

kiosk 130 can abort the transfer without writing the data to the secure area 142 of the SD card 140. As a result, no matter what portion of the media file has been downloaded to the SD card 140 prior to the transfer process being aborted, the customer will not be able to playback any playable content that was downloaded to the SD card” (Ex. 1001 at 9:65-10:7).

147. Thompson discloses that the programming process will only initiate after the user has confirmed the purchase: “Payment can be made either through the payment device on the video kiosk, or the cost of the video content can be deducted from the user’s account or automatically charged to a credit card on file. The control program and electronics 2300 can then retrieve the selected video content from the video content servers, and initiate the media programming process” (Ex. 1005 at [0117]).

148. A POSITA would have understood that in Thompson’s system, the secure key data would only be written to the memory device after successful payment and transaction completion, as this would ensure that users could not access content they had not properly purchased.

149. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara renders Claim 8 obvious to a POSITA at the time of the alleged invention.

i. Claim 10 Analysis

i. 10[pre]: The method of claim 7, further comprising:

150. As explained above, Thompson and Kasahara, alone or in combination, render obvious Claim 7.

ii. 10[a]: writing the user key to the secure area of the SD card prior in time to writing all data to the unsecure area of the SD card; and

151. Thompson and Kasahara, either alone or in combination, teach this claim limitation. Kasahara discloses that the SDSD user key data Kub (“user key”) is written to the protection area (“secure area”) of the SD card 20 before completion of initiation of the data transfer (Ex. 1007 at [0066]). After initiation, the SDSD content key data Kcib is encrypted with the user key and both are saved on the SD card 20 (Ex. 1007 at [0067]).

152. It would have been obvious to a POSITA to combine Kasahara’s encryption method (using a user key to encrypt a content key which encrypts content data), and writing the user key to the secure area of the SD card prior in time to writing all data to the unsecure area, with the system disclosed by Thompson. This approach ensures that the key needed to decrypt the content is securely stored before the encrypted content is written to the card.

iii. 10[b]: writing other data to the secure area of the SD card after in time writing all data to the unsecure area of the SD card.

153. For the same reasons explained for Claim 1[h], Thompson and Kasahara, alone or in combination, teach writing other data to the secure area of the SD card after writing all data to the unsecure area of the SD card.

154. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara renders Claim 10 obvious to a POSITA at the time of the alleged invention.

j. Claim 11 Analysis

i. 11[pre]: The method of claim 7,

155. As explained above, Thompson and Kasahara, alone or in combination, render obvious Claim 7.

ii. 11[a]: where the directory blocks are optionally written at once.

156. Thompson teaches this claim limitation. Thompson discloses that the data to be written may be divided into many portions, whereafter these portions are stored in sub-arrays, thus allowing for parallel writing of all information so stored (Ex. 1005 at [0072]).

157. Furthermore, it would have been obvious to a POSITA to write directory blocks of a media file all at once because writing directory blocks all at once ensures that file system metadata remains contiguous and consistent, reducing

fragmentation and increasing read/write performance. This was a standard practice in file system operations at the time of the alleged invention.

158. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara renders Claim 11 obvious to a POSITA at the time of the alleged invention.

k. Independent Claim 12 Analysis

i. 12[pre]: A non-transitory computer readable storage medium storing instructions thereon, the instructions when executed cause at least one processor to:

159. Thompson discloses a computer-readable storage medium that stores computer-readable program code. Specifically, Thompson discloses that the video kiosk comprises circuitry to control its operation, and the circuitry can comprise a computer-readable medium that stores computer-readable code (Ex. 1005 at [0043]).

ii. 12[a]: identify a media file for download to an SD card;

160. For the same reasons explained for Claim 7[a], Thompson and Kasahara, alone or in combination, teach identifying a media file for download to an SD card.

iii. 12[b]: pre-allocate space on the SD card for a playable content portion of the media file, wherein the playable content portion of the media file is encrypted by a content key that is encrypted by a user key;

161. For the same reasons explained for Claim 7[b], Thompson and Kasahara, alone or in combination, teach pre-allocating space on the SD card for a

playable content portion of the media file, wherein the playable content portion of the media file is encrypted by a content key that is encrypted by a user key.

- iv. 12[c]: write all directory blocks together of the playable content portion of the media file and, thereafter in time, write all data blocks sequentially of the playable content portion of the media file; and**

162. For the same reasons explained for Claim 7[c], Thompson and Kasahara, alone or in combination, teach writing all directory blocks together of the playable content portion of the media file and, thereafter in time, writing all data blocks sequentially of the playable content portion of the media file.

- v. 12[d]: write all data that is to be written to an unsecure area of the SD card, including the encrypted playable content, prior in time to writing any data to a secure area of the SD card, except for the user key.**

163. For the same reasons explained for Claim 7[d], Thompson and Kasahara, alone or in combination, teach writing all data that is to be written to an unsecure area of the SD card, including the encrypted playable content, prior in time to writing any data to a secure area of the SD card, except for the user key.

164. Based on my analysis of each limitation of Claim 12, it is my opinion that the combination of Thompson and Kasahara renders Claim 12 obvious to a POSITA at the time of the alleged invention.

l. Claim 13 Analysis

i. 13[pre]: The computer readable storage medium of claim 12,

165. As explained above, Thompson and Kasahara, alone or in combination, render obvious Claim 12.

ii. 13[a]: wherein, except for a user key, data is only written to the secure area of the SD card if a transaction for the media file successfully completes.

166. For the same reasons explained for Claim 8[a], Thompson and Kasahara, alone or in combination, teach that, except for a user key, data is only written to the secure area of the SD card if a transaction for the media file successfully completes.

167. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara renders Claim 13 obvious to a POSITA at the time of the alleged invention.

m. Claim 15 Analysis

i. 15[pre]: The computer readable storage medium of claim 12, further comprising instructions that when executed cause the at least one processor to:

168. As explained above, Thompson and Kasahara, alone or in combination, render obvious Claim 12.

- ii. 15[a]: write the user key to the secure area of the SD card prior in time to a write of all data to the unsecure area of the SD card; and**

169. For the same reasons explained for Claim 10[a], Thompson and Kasahara, alone or in combination, teach writing the user key to the secure area of the SD card prior in time to a write of all data to the unsecure area of the SD card.

- iii. 15[b]: write other data to the secure area of the SD card after in time a write of all data to the unsecure area of the SD card.**

170. For the same reasons explained for Claim 10[b], Thompson and Kasahara, alone or in combination, teach writing other data to the secure area of the SD card after in time a write of all data to the unsecure area of the SD card.

171. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara renders Claim 15 obvious to a POSITA at the time of the alleged invention.

n. Claim 16 Analysis

- i. 16[pre]: The computer readable storage medium of claim 12,**

172. As explained above, Thompson and Kasahara, alone or in combination, render obvious Claim 12.

ii. 16[a]: where the directory blocks are optionally written at once.

173. For the same reasons explained for Claim 11[a], Thompson and Kasahara, alone or in combination, teach that the directory blocks are optionally written at once.

174. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara renders Claim 16 obvious to a POSITA at the time of the alleged invention.

VIII. GROUND 2: CLAIM 4 IS OBVIOUS OVER THOMPSON AND KASAHARA IN VIEW OF WAGNER

a. Motivation to Combine Thompson, Kasahara, and Wagner

175. In my opinion, a POSITA would have been motivated to combine the teachings of Thompson, Kasahara, and Wagner for several reasons. All three references are directed toward improving the efficiency, security, and reliability of digital media transfer and distribution. Each reference addresses key aspects of content delivery through kiosks or similar systems that store and transmit digital media files to removable storage devices.

176. Wagner, like Thompson and Kasahara, is in the same field of endeavor of secure content delivery via automated kiosks and other media distribution terminals. Wagner specifically teaches advancements in content management that enhance the protection of the media content (Ex. 1006 at [0055]).

177. A POSITA would have recognized that integrating Wagner's techniques into the combined Thompson-Kasahara system would lead to a predictable and desirable improvement in digital media distribution, without requiring substantial modifications to the existing system. Given that Wagner's methods align with the objectives of Thompson and Kasahara, a POSITA would have understood that incorporating these features would have improved the overall performance of a kiosk-based content delivery system.

b. Claim 4 Analysis

i. 4[pre]: The kiosk of claim 1,

178. As explained above for Ground 1, Thompson and Kasahara, alone or in combination, render obvious Claim 1.

ii. 4[a]: further comprising a software player update module for transferring a software player update to the SD card.

179. Wagner teaches this claim limitation. Wagner discloses a kiosk that downloads required software onto a flash card: "customer places an order, using the system described above, for digital content, and downloads that digital content, **and any required software**, to the customer's PC or other playback device, or to a removable memory such as a CF or SD card, DVD, CD, USB flash drive, or the like at point-of-content-delivery 18" (Ex. 1006 at [0044] (emphasis added)).

180. Wagner further describes a mechanism for updating at least the programming of RAM memory 230, which can be used to update the functionality

of an adapter or to add or remove digital rights management functionality: “the RAM memory 230 may be updated with new features. For example, if a modification is made to a digital rights management (DRM) process, this update could be programmed into RAM 230 to implement the modifications. The RAM 230 may be updated by the playback device. This can be done if flash media 200 is connected directly to an Internet or otherwise connected computing device or device which itself has such Internet or equivalent connection and can thus download any software for the update” (Ex. 1006 at [0072]).

181. The specification of the '783 Patent does not mention a “software player update module”, however it explains that “[t]he firmware update module 138 receives firmware updates (e.g., firmware software updates). . . for use in updating firmware on the playback devices that use the SD cards 140.” Ex. 1001 at 5:17-21.

182. Thus, a POSITA would have understood that Wagner’s kiosk includes functionality for downloading software updates onto a flash card, which means that Wagner necessarily included the type of “software player update module” claimed in the '783 Patent.

183. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara in view of Wagner renders Claim 4 obvious to a POSITA at the time of the alleged invention.

IX. GROUND 3: CLAIMS 9 AND 14 ARE OBVIOUS OVER THOMPSON AND KASAHARA IN VIEW OF ISHIHARA

a. Motivation to Combine

184. In my opinion, a POSITA would have been motivated to combine the teachings of Thompson, Kasahara, and Ishihara for several reasons. All three references address key challenges in secure digital content distribution. Ishihara discloses a content protection mechanism specifically tailored for digital media, including encryption techniques, key management, and authentication protocols that prevent unauthorized access and copying.

185. Thompson teaches a kiosk-based system for transferring digital content to portable storage media, while Kasahara provides an encryption and secure content management framework for content delivery to SD cards. The combination of Ishihara's encryption methodologies with Thompson and Kasahara's content delivery model would have been an obvious improvement, ensuring enhanced data protection and controlled access to digital content.

186. A POSITA would have understood that integrating Ishihara's security framework into the Thompson-Kasahara system would provide multiple advantages. Ishihara describes a hierarchical encryption system where a memory public key is used to encrypt licenses, and a memory private key is required for decryption before playback. Ex. 1009 at 23, 26. This model ensures that only authorized users with valid licenses can access digital content, preventing unauthorized duplication.

187. Applying this encryption system to Thompson's kiosk model would have further strengthened its security, ensuring that purchased or rented digital media files could not be accessed without authentication. Kasahara's structured content encryption methods already complement Thompson's approach to digital media delivery, and adding Ishihara's licensing and key management framework would create a more comprehensive DRM system.

b. Claim 9 Analysis

i. 9[pre]: The method of claim 7,

188. As explained above for Claim 7, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 7.

ii. 9[a]: wherein the SD card is pre-configured with the user key stored in the secure area of the SD card.

189. Ishihara teaches this claim limitation. Ishihara discloses a secure memory card with pre-installed keys that provide security for content protection. Specifically, Ishihara states that "the unique key is derived from a random seed at production time, and then stored in a protected area on-board the memory card." Ex. 1009 at p. 23, 26. Ishihara further explains that "each licensed SMMC is manufactured with a unique device key," emphasizing that these keys are installed during manufacturing, not during content transfer. Ex. 1009 at p. 23, 26.

190. Incorporating Ishihara's pre-configuration of user keys into the Thompson-Kasahara system to streamline the authentication and decryption process

for media files would have been obvious to a POSITA. In the Thompson-Kasahara system, encryption keys are essential for content playback, and ensuring that a user key is pre-installed in the secure area of an SD card would simplify and enhance the user experience by eliminating the need for additional key transfers at the time of media download.

191. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara in view of Ishihara renders Claim 9 obvious to a POSITA at the time of the alleged invention.

c. Claim 14 Analysis

i. 14[pre]: The computer readable storage medium of claim 12,

192. As explained above for Claim 12, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 12.

ii. 14[a]: wherein the SD card is pre-configured with the user key stored in the secure area of the SD card.

193. For the same reasons described for Claim 9[a] above, Ishihara discloses this limitation.

194. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara in view of Ishihara renders Claim 14 obvious to a POSITA at the time of the alleged invention.

X. GROUND 4: CLAIMS 17 AND 18 ARE OBVIOUS OVER THOMPSON AND KASAHARA IN VIEW OF PONCELEON

a. Motivation to Combine

195. In my opinion, a POSITA would have been motivated to combine the teachings of Thompson, Kasahara, and Ponceleon for several reasons. Ponceleon provides additional details on secure digital media distribution models, including subscription and licensing mechanisms. Ex. 1008 at 496. Thompson and Kasahara already describe a secure digital content transfer system, but Ponceleon introduces sophisticated DRM frameworks that facilitate controlled access and rental-based digital media distribution. Ex. 1008 at 496.

196. Integrating Ponceleon's licensing and DRM structures with Thompson and Kasahara's secure kiosk-based delivery system would have been a natural extension of existing methods, providing an improved and commercially viable approach to digital media transactions.

197. A POSITA would have recognized that incorporating Ponceleon's user authentication and access control techniques would yield a predictable and beneficial enhancement to the secure digital kiosk environment of Thompson and Kasahara.

b. Claim 17 Analysis

i. 17[pre]: The computer readable storage medium of claim 12

As explained above for Claim 12, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 12.

ii. 17[a]: wherein the instructions cause the media file to be downloaded to the SD card in substantially 2 minutes.

198. Thompson and Ponceleon, either alone or in combination, teach this limitation. Thompson discloses a “high-speed programming port” that has a data transfer rate of between 65 MB/sec to 500 MB/sec. Ex. 1005 at [0047]. This rate would allow for the download of a typical movie file in just a few minutes.

199. Ponceleon discloses that, as of its publishing, there were systems using SD cards to achieve the download of a 120-minute movie in less than 20 seconds.

200. At these transfer rates, even large media files could easily be downloaded to an SD card in substantially 2 minutes or less.

201. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara in view of Ponceleon renders Claim 17 obvious to a POSITA at the time of the alleged invention.

c. Claim 18 Analysis

i. 18[pre]: The method of claim 7

202. As explained above for Claim 7, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 7.

ii. 18[a]: wherein the media file is downloaded to the SD card in substantially 2 minutes.

203. For the same reasons described for Claim 17[a] above, Thompson and Ponceleon, either alone or in combination, teach this limitation.

204. Based on my analysis, it is my opinion that the combination of Thompson and Kasahara in view of Ponceleon renders Claim 18 obvious to a POSITA at the time of the alleged invention.

XI. SUMMARY OF CONCLUSIONS

205. Based on my analysis of the '783 Patent and the prior art, I conclude that the claimed invention would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. The combination of Thompson and Kasahara renders Claims 1-3, 5-8, 10-13, 15, and 16 obvious. The combination of Thompson, Kasahara, and Wagner renders Claim 4 obvious. The combination of Thompson, Kasahara, and Ishihara renders Claims 9 and 14 obvious. The combination of Thompson, Kasahara, and Ponceleon renders Claims 17 and 18 obvious.

206. As discussed above, I have been informed that secondary considerations are a factor in the determination of obviousness. I have considered the current information related to secondary considerations of obviousness and determined that it has no impact on my conclusions. To the extent patent owner comes forward with any additional information, I will consider it.

207. This declaration represents the opinions on the '783 Patent that I have formed to date. I reserve the right to revise, supplement, and/or amend my opinions stated herein based on new information that becomes available to me and on my

continuing analysis of the materials already provided. In connection with any arguments raised by patent owner, opinions by patent owner's expert(s), additional evidence and testimony, and/or judicial determinations, whether in this or a related proceeding, I reserve the right to supplement my opinions in the future to respond thereto.

I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct, that all statements made of my own knowledge are true, and that all statements made on information and belief are believed to be true. I understand that willful false statements are punishable by fine or imprisonment or both pursuant to 18 U.S.C. § 1004.

Dated: March 12, 2025

A handwritten signature in blue ink, appearing to read "R. J. Baker", is written over a horizontal line.

R. Jacob Baker, Ph.D., P.E.