

The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board

Paper No. 18

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte STEPHEN T. WONG
and JAMES YUAN-PIN YU

Appeal No. 2001-0575
Application 08/924,867

ON BRIEF

Before THOMAS, KRASS , and JERRY SMITH, Administrative Patent Judges.

KRASS, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal from the final rejection of claims 1-3, 5-9, 11-15 and 17-21, all of the pending claims.

The invention is directed to a digital trust center for medical image authentication. In particular, systems exist for management of image information including digital images and associated data by maintaining at least one central electronic archive which may be accessed over a digital data network. A system known as Picture Archiving and Communications Systems

(PACS) is used for medical images in association with a digital trust center for enabling authentication of the image information. In order to protect the confidentiality of the information and determine the authenticity of digital images, cryptographic techniques have been integrated with PACS. By employing a digital trust center, an authentication server is provided to attach a hash value, i.e., a “digital fingerprint,” derived from the image data set to an incoming image dataset so that the hash is stored with the image data set in the image data store maintained by the PACS archive server. The PACS archive server can check the authenticity of the image data set by comparing the stored hash with one it computes from the stored image data set.

In order to reduce vulnerability of such a system to attack or a comprise of authenticity and security, the invention provides “in association with an image management system, an authentication and security system comprising an authentication server or so-called “digital trust center” which maintains and stores hashes and corresponding time stamps indicating the times of receipt of the respective hashes, and provides them on request in encrypted form, and further functionality in the image acquisition computers and the display stations to provide for security and to interact with the authentication server for authentication purposes” [specification-page 4].

Independent claim 1 is reproduced as follows:

1. In an image management system comprising image acquisition computers for acquiring image information from imaging devices associated with the image acquisition computers and forming image datasets, each comprising an image header and image data, an image archive server for receiving the image datasets from the acquisition computers and maintaining at least one image data store for the image datasets, and a plurality of remote display stations for displaying images from requested image datasets which are retrieved by the image archive server from the image data store and sent to the requesting display station, an authentication and security system comprising:

an authentication server for maintaining and storing pairs of hashes and identifiers, and for providing hashes in encrypted form in response to requests from display stations, wherein the requests include identifiers;

the acquisition computers being configured for pre-processing the image datasets, including performing any required image compression, encrypting at least a portion of the image datasets after any such compression, forming identifiers, computing hashes, providing pairs of hashes and identifiers to the authentication server, and sending pre-processed image datasets to the image archive server for storage in the image data store; and

the display stations being configured for requesting and receiving identified pre-processed image datasets from the image archive server, decrypting the image datasets sent by the image archive server, performing any required data decompression on the image datasets, forming identifiers from the image datasets, computing hashes from the image datasets, sending requests including the formed identifiers to the authentication server, receiving identified hashes in encrypted form from the authentication server, decrypting hashes received from the authentication server, and comparing the hashes obtained from the authentication server with the hashes computed locally from the image datasets received from the image archive server.

The examiner relies on the following references:

Fisher et al. (Fisher)	4,833,625	May 23, 1989
Dyson	5,050,212	Sep. 17, 1991
Haber et al. (Haber)	5,136,647	Aug. 4, 1992
Conner et al. (Conner)	5,579,393	Nov. 26, 1996

Claims 1-3, 5-9, 11-15 and 17-21 stand rejected under 35 U.S.C. § 103. As evidence of obviousness, the examiner cites Fisher and Dyson with regard to claims 1 and 21, adding Haber with regard to claims 2, 3, 5 and 6, and further adding Conner with regard to claims 7-9, 11-15 and 17-20.

Reference is made to the brief and answer for the respective positions of appellants and the examiner.

OPINION

With regard to the independent claim, the examiner provides Fisher as a general teaching of a PACS system, but admits that Fisher does “not disclose either authenticating the images, securing the transmission of the images through encryption, data compression, or image datasets comprising an image header and image data” [answer-page 4]. The examiner then turns to Dyson for a teaching of storing a pre-computed hash (the first identifier, at column 3, lines 36-42) locally on a computer, acknowledging the advantage of broadcasting a file from separate storage locations across the communication network to many computers simultaneously, at column 2, lines 46-56. The examiner then spends pages 5-7 of the answer, delineating the many failures of Dyson and conjecturing on why so many of the missing claim limitations would have been obvious to the artisan and how and why the combination of Fisher/Dyson would have allowed for secured transmission through encryption and authentication of medical images in the form of image datasets and would have provided certain benefits, without any specific evidence to support those allegations.

Clearly, the examiner has not established a prima facie case of obviousness with regard to the instant claimed subject matter.

While the following is not meant to be an exhaustive list of deficiencies in the examiner’s case, it will suffice to show some of the errors in the examiner’s reasoning:

Claim 1 calls for an “image archive server” and recites how it is functionally intertwined with other claimed elements. The examiner appears to agree that the applied references fail to

show such an image archive server, contending merely that it would be “advantageous for the pre-computed hashes to be stored in a central archive controlled by a server rather than each computer [as taught by Dyson] having to store the pre-computed hashes separately because it would not necessitate that each display computer devote its [sic] limited system resources to storing hashes. It would have been obvious...to include a server controlling a storage device in which pre-computed hashes would be placed and call that an authentication server” [answer-page 5]. The examiner has no reasonable basis for this conclusion as the applied references clearly do not teach or suggest a central “archive server,” as claimed. The examiner has offered no evidence that there would have been any advantage to storing pre-computed hashes in a central archive controlled by a server and it would appear that the only evidence of this, on the record, is appellants’ own disclosure.

While it is not clear what the examiner relies on for the teaching of the claimed “acquisition computers” and the “display stations,” the examiner’s statement that a “single computer *could* serve as both an acquisition and/or display computer” [answer-page 5-emphasis added] falls far short of an evidentiary showing of obviousness since the mere fact that something *could* be done does not, in and of itself, constitute obviousness within the meaning of 35 U.S.C. § 103.

While the examiner admits that Dyson does not teach the advantages of including an identifier with the hash, the examiner concludes that it would have been obvious to include such an identifier because, “without the identifier, it would be difficult to know which hash belongs to

which data” [answer-page 6]. Again, the examiner makes an allegation but fails to point to anything to support such an allegation. If Dyson disclosed a hash without an identifier, then, clearly, all hashes must not need such an identifier. Accordingly, the examiner must show some reason, suggested by the prior art, as to why the artisan would have been led to supply such identifiers where none are taught.

Further, the examiner alleges that although Dyson fails to teach the advantages of encrypting the pre-processed hashes and having the display computer decrypt the hash which was received from the authentication server, it would have been obvious to include an encryption module in the authentication server to encrypt hashes because Dyson equips each computer with encryption/decryption modules. How can it possibly be obvious to encrypt hashes received from an authentication server when there is no authentication server taught by the applied references? The examiner’s rationale appears to be nothing more than a bevy of unsupported obviousness conclusions based on previous, bootstrapped, unsupported conclusions of obviousness.

The examiner’s entire case is comprised of unsupported allegations of what would have been “obvious” or “advantageous.” Even if certain things might have been well known, there must still be some convincing reasoning as to what would have motivated the artisan to make the proposed modifications. This factual question of motivation is material to patentability, and cannot be resolved on subjective belief and unknown authority. It is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to “[use] that which the inventor taught against its teacher.” In re Sang-Su Lee, 277 F.3d 1338,

Appeal No. 2001-0575
Application 08/924,867

61 USPQ2d 1430 (Fed. Cir. 2002). When the examiner relies on what is asserted to be general knowledge to negate patentability, that knowledge must be articulated and placed on the record. We cannot rely on conclusory statements when dealing with particular combinations of prior art and specific claims. In re Sang-Su Lee.

Even assuming, arguendo, that much of what the examiner alleges is true, there appears to be no cogent rationale set forth as to why the artisan would have combined the PACS system teachings of Fisher with Dyson which is concerned with verifying the integrity of a file stored separately from a computer. There is nothing to suggest any use for Dyson's storage of verifying information in a centralized archive server.

Since neither Haber nor Conner provides for any of the deficiencies, as noted supra, in the examiner's case, the rejections based on these references in combination with Fisher and Dyson must also fall.

Appeal No. 2001-0575
Application 08/924,867

The examiner's decision rejecting claims 1-3, 5-9, 11-15 and 17-21 under 35 U.S.C.

§ 103 is reversed.

REVERSED

James D. Thomas)	
Administrative Patent Judge)	
)	
)	
)	
Errol A. Krass)	BOARD OF PATENT
Administrative Patent Judge)	APPEALS AND
)	INTERFERENCES
)	
)	
Jerry Smith)	
Administrative Patent Judge)	

EAK/cam

Dwight H. Renfrew, Jr.
C/O U.S. Philips Corp.
Intellectual Property Dept.
580 White Plains Road
Tarrytown, NY 10591