The opinion in support of the decision being entered today is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

---

*Ex parte* MICHAEL E. BAZAKOS,
RIDHA M. HAMZA,
and DAVID W. MEYERS

---

Appeal 2007-1736
Application 10/979,129[1]
Technology Center 2600

---

Decided: August 6, 2007

---

Before ANITA PELLMAN GROSS, JAY P. LUCAS,
and JOHN A. JEFFERY, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134 from the Examiner's rejection of claims 1-3, 5-15, and 17-27.[2] Claims 4 and 16 have been

[1] This application is a continuation-in-part of U.S. Pat. Application Ser. No. 10/655,124, filed Sept. 5, 2003, now U.S. Pat. 7,183,895 B2.

indicated as containing allowable subject matter (Answer 15-16). We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

## STATEMENT OF THE CASE

Appellants invented a dynamic security verification system that verifies data read from a radio frequency identification (RFID) tag at two different checkpoints. At a first checkpoint, data from an RFID tag is read and used to retrieve a face print corresponding to information associated with the RFID tag from a database. A facial image is then obtained and compared with the retrieved face print.

At a second checkpoint, the RFID tag is re-read and this information is compared with the information obtained at the first checkpoint. This comparison provides a post-verification check to ensure the RFID data matches. Claim 1 is illustrative:

1. A method for providing dynamic security verification, comprising:

storing data regarding information and a face print of a person in a database, wherein the face print is represented by numerical codes of a face image of the person;

at a first checkpoint, reading an RFID device and relating a read RFID number to the information stored in the database, retrieving a face print corresponding to the RFID device from the database;

---

[2] Although Appellants indicate that the Examiner's Final Rejection of claims 1-27 is under appeal, the Examiner had indicated that claims 4 and 16 contain allowable subject matter. *See* Final Rejection, at 6; *see also* Answer, at 15-16. In any event, the grounds of the Examiner's obviousness rejection in the Final Rejection were changed in the Answer to withdraw the Mays reference in connection with the rejection of claims 1, 3, (not 1-3 as the Examiner indicates on Page 3 of the Answer) 5-8, 17-21, 25, and 26 (Answer 3).

scanning a face of the person to obtain a facial image;

comparing the facial image with the retrieved face print; and

at a second checkpoint, re-reading the RFID device and comparing the re-read RFID device with the information read at the first checkpoint.

The Examiner relies on the following prior art references to show unpatentability:

| | | |
|---|---|---|
| Suzuki | US 5,801,763 | Sep. 1, 1998 |
| Mays | US 6,275,157 B1 | Aug. 14, 2001 |
| Ritter | US 6,657,538 B1 | Dec. 2, 2003 (filed Sep. 28, 1999) |
| Calvesio | US 6,867,683 B2 | Mar. 15, 2005 (filed Dec. 28, 2000) |

1. Claims 1, 3, 5-8, 17, 18, 20, 21, 25, and 26 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Calvesio in view of Ritter.
2. Claims 2, 9-15, 19, and 22-24 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Calvesio in view of Ritter and further in view of Mays.
3. Claim 27 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Calvesio in view of Ritter and further in view of Suzuki.

Rather than repeat the arguments of Appellants or the Examiner, we refer to the Briefs and the Answer for their respective details. In this decision, we have considered only those arguments actually made by Appellants. Arguments which Appellants could have made but did not make in the Briefs have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

OPINION

*Claims 1, 3, 5-8, 17, 18, 20, 21, 25, and 26*

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See In re Fine*, 837 F.2d 1071, 1073, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). In so doing, the Examiner must make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (1966).

Discussing the question of obviousness of a patent that claims a combination of known elements, the Court in *KSR Int'l v. Teleflex, Inc*., 127 S. Ct. 1727, 82 USPQ2d 1395 (2007) explains:

> When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, §103 likely bars its patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill. *Sakraida* [*v. AG Pro, Inc.*, 425 U.S. 273, 189 USPQ 449 (1976)] and *Anderson's-Black Rock*[, *Inc. v. Pavement Salvage Co*., 396 U.S. 57, 163 USPQ 673 (1969)] are illustrative—a court must ask whether the improvement is more than the predictable use of prior art elements according to their established functions.

*KSR*, 127 S. Ct. at 1740, 82 USPQ2d at 1396. If the claimed subject matter cannot be fairly characterized as involving the simple substitution of one known element for another or the mere application of a known technique to a piece of prior art ready for the improvement, a holding of obviousness can be based on a showing that "there was an apparent reason to combine the

known elements in the fashion claimed." *Id.*, 127 S. Ct. at 1740-41, 82 USPQ2d at 1396. Such a showing requires "some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. . . . [H]owever, the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ." *Id.*, 127 S. Ct. at 1741, 82 USPQ2d at 1396 (quoting *In re Kahn*, 441 F.3d 977, 987, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006)).

If the Examiner's burden is met, the burden then shifts to the Appellants to overcome the prima facie case with argument and/or evidence. Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments. *See In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992).

Regarding representative claim 1,[3] the Examiner's rejection essentially finds that Calvesio teaches a security system with every claimed feature including a general teaching of verifying an individual's facial characteristics for security purposes. The Examiner, however, notes that Calvesio does not disclose the specific method used for such facial recognition, namely (1) retrieving facial images from a facial recognition reader, (2) retrieving stored facial templates from a database, and (3) comparing the processed facial images with the stored facial template as claimed. The Examiner cites Ritter as teaching these features and concludes

[3] Appellants argue claims 1-3 and 6-8 together as a group. *See* Br. 5-6. Accordingly, we select claim 1 as representative. *See* 37 C.F.R. § 41.37(c)(1)(vii).

that it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate such facial recognition features in Calvesio to authenticate an individual (Answer 4-5).

Appellants argue that the prior art does not teach comparing the data from the first checkpoint with the data read at the second checkpoint (Br. 5-6). The Examiner responds that Calvesio's monitoring of a person's egress within a secured facility involves verifying a person's identity at the entrance and exit (i.e., verifying that the same person entered and left the security zone). According to the Examiner, such a verification would inherently include comparing the individual's identity at the entrance and exit (Answer 16-17).

Appellants argue that it is not inherent that Calvesio checks data read at one checkpoint when reading data at another checkpoint, particularly in view of the reference's emphasis on tracking people with a central database. Appellants add that there is no need to check previously read data in Calvesio since, among other things, Calvesio assumes anyone at an exit is properly in the secured area they are leaving (Reply Br. 2-3).

We will sustain the Examiner's rejection of representative claim 1. Calvesio discloses a high security identification system that controls access to various zones within a secured facility. As shown in Figure 5, the facility (FAC1) is divided into five zones. After the individual enters the facility by passing through Gate G1 and the guard desk, entry to each respective zone is controlled by restricting passage through doors G2-G7 via corresponding card readers R2-R7 that are also associated with a biometric measuring facility (Calvesio, col. 7, l. 40 – col. 8, l. 3; Fig. 5).

In our view, Calvesio strongly suggests comparing data obtained from one checkpoint with another. As the Examiner indicates, monitoring the egress of a particular individual throughout a secured facility (Calvesio, col. 8, ll. 4-44) would, at a minimum, involve identifying that individual at each entrance and exit. To track a particular individual's whereabouts, the system must first obtain the identity of a particular individual, and then verify the identity of *that individual* every time a card is swiped (i.e., when entering a zone).

Such tracking, in our view, strongly suggests comparing the identity of the individual for every card swipe at least with respect to the identity data obtained at the initial checkpoint. That is, data obtained at the initial checkpoint (i.e., the guard desk) would inform the system that a particular individual has entered the secured facility. Following this initial data input, any subsequent egress monitoring would, at least implicitly, involve comparing the identity of the individual who initially entered the facility with the identity information subsequently obtained at each respective zone.

Calvesio provides further evidence of comparing data from different checkpoints. Specifically, Calvesio notes that an access violation can occur if an individual somehow exits a zone without swiping a card or otherwise providing an event that records leaving the zone in the system. As an example, Calvesio notes that if the system indicates that the individual is in Zone 2, but seeks passage into Zone 5, both the local guard and the enrollment facility should receive automated notification from the computer equipment at the door to Zone 5 (Calvesio, col. 10, ll. 42-65).

As shown in Figure 5, an individual in Zone 2 cannot enter Zone 5 without first passing through Zones 3 and 4. To enter Zone 5, the individual

must be in Zone 4. *See* Calvesio, Fig. 5. For clarity, the relevant information that would indicate this passage from Zones 4 to 5 is summarized below:

| Individual | Current Zone | Exiting Zone | Entering Zone |
|---|---|---|---|
| John Doe | 4 | 4 | 5 |

Table 1: Summary of Information Indicating Passage From Zone 4 to 5

As Table 1 indicates, at least the "Current Zone" and "Exiting Zone" data must match to allow passage to Zone 5. Otherwise, an access violation occurs and a corresponding notification is generated.[4] Table 2 summarizes the relevant information corresponding to this situation commensurate with Calvesio's example noted above:

| Individual | Current Zone | Exiting Zone | Entering Zone |
|---|---|---|---|
| John Doe | 2 | 4 | 5 |

Table 2: Summary of Information Indicating Access Violation

Thus, in order to determine whether an access violation occurs, Calvesio's system in effect compares "Current Zone" data with "Exiting Zone" data. If a mismatch occurs, an alarm signal is generated. In making this assessment, the "Current Zone" data would have been obtained from a

[4] *See* Calvesio, at col. 10, ll. 51-57.

previous checkpoint (i.e., at the entrance to that zone), while the "Exiting Zone" and "Entering Zone" data would have been obtained from a subsequent checkpoint.

Therefore, not only does this functionality strongly suggest the comparison recited in claim 1, but also the mismatch alarm signal recited in claim 5.[5]

In addition, Calvesio notes that if an individual is approved to pass through more than one security door at a given time and is approved for travel through a particular portal, the system may also check to determine whether this individual is recorded as *present in another location at the same time* (Calvesio, col. 5, ll. 59-63) (emphasis added). In our view, such a check for simultaneous presence in different locations would reasonably involve comparing the location and identity information at the current checkpoint (i.e., at the approved portal) with such information obtained from other checkpoints.

For at least these reasons, we find Calvesio amply suggests comparing data read at one checkpoint with data read at another checkpoint as recited in claim 1 and the alarm signal indication of claim 5. Moreover, Appellants have not persuasively rebutted the Examiner's reliance on the secondary reference to Ritter and its combination with Calvesio – a position that we find reasonable.

We therefore sustain the Examiner's rejection of representative claim 1 and claim 5. Likewise, we sustain the Examiner's rejection of claims 3 and 6-8 which fall with claim 1.

[5] *See id.*

*Claims 9-15*

Regarding representative claim 9,[6] Appellants argue that the prior art does not disclose comparing data read at first and second sensing points to determine if the data matches (Br. 7). For the reasons previously discussed, however, we find Calvesio amply suggests this limitation and the reference is reasonably combinable with Ritter.[7] Since Appellants have not persuasively rebutted the Examiner's prima facie case of obviousness, the rejection of claims 9-15 is sustained.

*Claims 17-26*

Regarding representative claim 17,[8] Appellants argue that the prior art does not disclose comparing data read at first and second verification devices is compared at a computer as claimed (Br. 8). For the reasons previously discussed, however, we find Calvesio amply suggests this limitation and the reference is reasonably combinable with Ritter.[9] Since Appellants have not persuasively rebutted the Examiner's prima facie case of obviousness, the rejection of claims 9-15 is sustained.

*Claim 27*

Likewise, we will sustain the Examiner's rejection of claim 27 under 35 U.S.C. § 103(a) as being unpatentable over the teachings of Calvesio in view of Ritter and further in view of Suzuki. We find that (1) the Examiner

---

[6] Appellants argue claims 9-15 together as a group. *See* Br. 7. Accordingly, we select claim 9 as representative.
[7] *See* p. 6-9, *supra*, of this opinion.
[8] Appellants argue claims 17-26 together as a group. *See* Br. 8. Accordingly, we select claim 17 as representative.
[9] *See* p. 6-9, *supra*, of this opinion.

has established at least a prima facie case of obviousness for these claims on Pages 14 and 15 of the Answer, and (2) Appellants have not persuasively rebutted the Examiner's prima facie case, but merely noted that the addition of Suzuki fails to cure the deficiencies of the other cited prior art in connection with claim 17. For the reasons previously discussed, however, the rejection is therefore sustained.

## DECISION

We have sustained the Examiner's rejections with respect to all claims on appeal. Therefore, the Examiner's decision rejecting claims 1-3, 5-15, and 17-27 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

KIS

HONEYWELL INTERNATIONAL INC.
101 COLUMBIA ROAD
P. O. BOX 2245
MORRISTOWN, NJ 07962-2245