

The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.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. 13

UNITED STATES PATENT AND TRADEMARK OFFICE

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Ex parte ALBERTO FERNANDEZ

Appeal No. 2004-0007
Application No. 09/844,105

ON BRIEF

Before FRANKFORT, NASE and BAHR, Administrative Patent Judges.
BAHR, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal from the examiner's final rejection of claims 1-4 and 26-43, which are all of the claims pending in this application.

We REVERSE and REMAND.

BACKGROUND

The appellant's invention relates to a system for electronically storing and retrieving value related information on a portable card (specification, page 1). As a security feature, appellant's system also stores a reference fingerprint corresponding to

numerical representations of the levels of charges trapped in the memory cells in which the value related information is stored (specification, page 12). As more fully explained in U.S. Pat. No. 5,644,636, issued to appellant on July 1, 1997 and incorporated by reference into the present application, previous levels of trapped charges for the memory cell and the total number of write cycles applied to the memory cell, known as the history of the memory cell, contribute to the pattern of the trapped charges in memory cells. Thus, the pattern of the trapped charges in memory cells of a memory array will vary randomly with each programming event, even when the same memory cell is programmed with the identical data (see column 4, lines 9-17 of the Fernandez patent). This stored reference fingerprint can then be compared with the pattern of trapped charges in the memory cells of the portable card when the card is presented for use in a transaction. If the stored and actual reference fingerprints do not match, the transaction will be refused. Appellant's system "protects against counterfeiting and provides for a high level of confidence in the integrity of the data without the need for complicated and expensive communications systems to verify each individual transaction" (specification, page 6). A copy of the claims under appeal is set forth in the appendix to the appellant's brief.

The examiner relied upon the following prior art references of record in rejecting the appealed claims:

Johnson	5,598,474	Jan. 28, 1997
Yamaguchi et al. (Yamaguchi)	6,314,196	Nov. 6, 2001 (filed Mar. 7, 1997)

The following is the sole rejection before us for review.

Claims 1-4 and 26-43 stand rejected under 35 U.S.C. § 103 as being unpatentable over Yamaguchi in view of Johnson.

Rather than reiterate the conflicting viewpoints advanced by the examiner and the appellant regarding the above-noted rejection, we make reference to the answer (Paper No. 9) for the examiner's complete reasoning in support of the rejection and to the brief and reply brief (Paper Nos. 8 and 10) for the appellant's arguments thereagainst.

OPINION

In reaching our decision in this appeal, we have given careful consideration to the appellant's specification and claims, to the applied prior art references, and to the respective positions articulated by the appellant and the examiner. For the reasons which follow, we cannot sustain the examiner's rejection.

Yamaguchi discloses a fingerprint registering and checking device and method which registers fingerprints and reads the fingerprints to see if the fingerprint is registered in the system. If the fingerprint is registered in the system, the system provides access to the user presenting the fingerprint. Such access can be in the form of unlocking a door lock, for example. In storing the fingerprint data, Yamaguchi's system also stores a key number, to or from which the contents of the n-th byte of the stored fingerprint data is added or subtracted to produce a conversion key number. The conversion key number is then inserted in the m-th byte of the fingerprint data. To

ensure the authenticity of the stored data, the contents of the n-th byte are then subtracted from or added to the conversion key number to reconstruct the key number. The reconstructed key number is then compared with the entered key number to determine whether the data is authentic.

Johnson discloses a process including the steps of reading a biological characteristic, such as a fingerprint, deciphering it and converting it to a unique number, and encrypting the unique number onto an ID card, such as an ATM card. When the card is used, the user's fingerprint is read by a reader, which then decipheres the fingerprint and compares the result to the encrypted number to determine if the user is an authorized user.

With respect to independent claims 1, 26, 35 and 41, the examiner has determined that "Yamaguchi does not disclose a read unit for reading the value information and reading the reference fingerprint to determine if the value information is authentic (which is equivalent to a process of authenticating a fingerprint or encrypting a fingerprint)" (answer, pages 4, 5 and 6) and that it would have been obvious "to modify the fingerprint registering of Yamaguchi by including the process for encrypting a fingerprint taught by Johnson because such modification would ensure that the transaction is carried out by the legal owner of the memory card" (answer, pages 4, 5 and 6). Even assuming that the modification proposed by the examiner were made to Yamaguchi's system, such modification would not address the feature (a read unit for reading the value information and reading the reference fingerprint to determine if the

value information is authentic) found by the examiner to be lacking. Moreover, inasmuch as the Yamaguchi system is directed to registering and checking fingerprints and granting access only to persons having fingerprints which are registered in the system and not to determining whether a person presenting a card is the legal owner of that card, the examiner's stated rationale for the modification does not appear to have any relevance to the Yamaguchi system. Furthermore, in any event, the read unit addressed by the examiner is recited in claims 26 and 35¹ but is not recited in claim 1. Rather, claim 1 recites a plurality of read/write units each being adapted to store and retrieve data from the solid-state media and to read and write authentication information in the form of an actual and an expected reference fingerprint from and to the solid-state media. The examiner's rejection does not address this feature.

It should be apparent from the above that we cannot sustain the examiner's rejection of independent claims 1, 26, 35 and 41, or claims 2-4, 27-34, 36-40, 42 and 43 depending therefrom, on the basis of the rationale offered by the examiner. The examiner's rejection is reversed.

REMAND TO THE EXAMINER

This application is remanded to the examiner, pursuant to our authority under 37 CFR § 41.50(a)(1), to review the scope of the claims and determine the differences, if any, between the claimed subject matter and the disclosure of Yamaguchi, in light of our

¹ Method steps of reading the value information from the transportable solid state media and reading the reference fingerprint and determining if the value information is authentic using the reference fingerprint are recited in claim 41.

observations regarding the claims and Yamaguchi, infra. If the examiner determines that there are no differences between Yamaguchi and the subject matter of any of appellant's claims, the examiner should reject such claims under 35 U.S.C. § 102. If the examiner identifies differences, the examiner should consider whether such differences are of such a nature that the subject matter as a whole would have been obvious in light of Yamaguchi in view of other prior art.

With particular regard to claim 1, we note that the solid-state media are recited simply as being "adapted for" storage of a reference fingerprint representing characteristics of the media created by an instance of writing data to the media. The examiner should consider whether this requires anything more than a conventional semiconductor memory device, such as an EEPROM, whose characteristics could be used as a basis for creating a reference fingerprint and which is capable of storing such reference fingerprint. We observe that all data stored in conventional EEPROMs, for example, is broadly representative of the level of charges trapped in the floating gates thereof, a characteristic of the media.

With further regard to claim 1, there is no indication on the record as to how the examiner is interpreting "stored value." Under its broadest interpretation, any data, in the form of "1" or "0" or stored charge or voltage is "stored value." It appears from the nature of the examiner's rejection and appellant's argument, however, that the examiner and appellant may be interpreting this terminology more narrowly. The interpretation given to this terminology should be made clear on the record.

It is also not clear how the examiner is interpreting “an actual and an expected reference fingerprint” as used in claim 1 and whether the recitation of the plurality of read/write units requires anything more than a broad read/write capability. As noted above, the claim language alluded to by the examiner as lacking in Yamaguchi with regard to the read unit is not recited in claim 1, implying that the examiner may not have fully come to grips with the scope of the recitation of the read/write units in claim 1.

Yamaguchi discloses a data authentication mechanism not discussed by either the examiner or appellant which appears to be quite pertinent to the subject matter of appellant’s claims. As explained in column 15, line 30, et seq., a key number is entered with the fingerprint data in the key setting register of the storage device² and the content of the n-th byte of the registered fingerprint data is added to or subtracted from the key number to produce a conversion key number which is inserted in the m-th byte of the registered fingerprint data. At the time of checking fingerprints, the content of the n-th byte is then subtracted from or added to the content of the m-th byte (the conversion key number) to reconstruct the key number. The reconstructed key number is then compared with the entered key number to ensure that the fingerprint data has not been altered since the key number was entered. Inasmuch as the data in the bytes of the fingerprint data are related in some fashion to the levels of charges trapped in the memory cells of the data storage device, the conversion key number inserted in the

² As explained in column 7, lines 6-11, the data storage device could be the storage unit 414, a hard disk drive in the host computer or an IC card 431 or optical card.

m-th byte is also related broadly to the level of charges trapped in the memory cells.

The examiner should thus determine whether this relationship is sufficient to satisfy the language in claim 1 “representing characteristics of the media created by an instance of writing data to the media” and the language in claims 26, 35 and 41 “representing measured levels of charges trapped in said memory cells.”

CONCLUSION

To summarize, the decision of the examiner to reject claims 1-4 and 26-43 under 35 U.S.C. § 103 is reversed and the application is remanded to the examiner for the reasons discussed above.

REVERSED AND REMANDED

CHARLES E. FRANKFORT)	
Administrative Patent Judge)	
)	
)	
)	
)	
)	BOARD OF PATENT
JEFFREY V. NASE)	APPEALS
Administrative Patent Judge)	AND
)	INTERFERENCES
)	
)	
)	
JENNIFER D. BAHR)	
Administrative Patent Judge)	

Appeal No. 2004-0007
Application No. 09/844,105

Page 10

Priest & Goldstein PLLC
5015 Southpark Drive
Suite 230
Durham, NC 27713-7736