User Identification Method based on Head Shape using a Helmet with Pressure Sensors

ABSTRACT

Helmets are used for various purposes such as industrial protective hat (work helmet), motorcycle helmet, sports helmet, and military/police helmet. If the wearer is known through wearing a shared helmet, name, affiliation, qualification can be shown on a display mounted on the helmet, and sensor data collected through helmet such as acceleration data, video, eye track data can be labeled with wearer's ID. In this paper, we propose a user identification and authentication method based on the user's head shape using a helmet equipped with 32 pressure sensors. We have implemented a prototype helmet device and captured data from nine subjects, resulting in 100% accuracy for user identification and 0.076 average EER for user authentication.

KEYWORDS

User identification, pressure sensor, helmet, head shape

ACM Reference Format:

. 2020. User Identification Method based on Head Shape using a Helmet with Pressure Sensors. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Helmets are used for various purposes such as industrial protective hat (work helmet), motorcycle helmet (bike, car, bicycle, etc.), sports helmet (American football, baseball, ice hokey, etc.), and military/police helmet. These are all worn to protect the head in the event of an accident[2]. It is considered important from a safety point of view that there is no gap between the head and the helmet.

Workers in factories and disaster sites have to wear helmets. There are also various people who do not know each other, such as short-term workers and vendors. If these people have own helmet, the wearer's name and work division are shown on the helmet, allowing the helmet wearer to be identified from a distance or overhead even if the wearer's face cannot clearly be seen. Identifying individuals is a deterrent to trespassers. In addition, showing the qualifications such as a hazardous materials engineer's license and heavy machinery licence helps create a safe work environment. In many cases, such information is directly written on the helmet or an identifiable sticker is attached to the helmet. However, in such an analog operation, it is easy for a trespasser to disguise himself by writing or stealing a sticker. Moreover, even if the worker mistakenly puts on other people's helmet, wrong information is displayed. If the helmets are shared among the workers, generally the helmet is not marked with the identifiable information.

In this paper, we propose a method that identifies and authenticates users based on the shape of their heads by installing pressure sensors inside a helmet. We implemented a prototype helmet with 32 pressure sensors. Our method compares the wear's data and registered users' data and identifies/authenticates the user.

The prototype helmet has a display to show user's name and credentials upon the identification result, therefore, wrong information is not displayed on the helmet if a helmet of someone else is used. It is useful that the identification information is automatically displayed on a shared helmet and workers can recognize each other. In addition, another advantage of user identification is data annotation. Data collected through sensors attached to the helmet or wears' body such as a camera, an eye tracker, and an accelerometer can automatically be annotated with the wear's ID. By attaching a GPS or an antenna to localize the user[11], the name and location of the worker can be determined in real time and it will be easier for the foreman to understand the overall situation in the field. Furthermore, from the pressure data between the helmet and the head, it is possible to check whether the shape of the head matches the helmet as zero pressure value means that there is a gap between the helmet and the head. Another possible use of the proposed helmet is a key for the door where access to the room is restricted according to the position or qualifications.

2 RELATED WORK

2.1 User Authentication Method

There are several methods to identify individuals: password, PIN, and stroke pattern; physical characteristics such as face, fingerprint, voice print, and iris; and behavioral characteristics such as handwriting and gait. Password, PIN, and stroke pattern that can be freely set by individuals have a risk of spoofing by shoulder hacking, brute force attack, and password duplication.

For physical characteristics, Chen et al.[4] use user's face and fingertips video images captured from the front and rear cameras of a mobile device. Siddharth et al.[1] use palm print and palm vein. Sayo et al.[13] use the shape of the lips and the movement of the lips during speech. Kim et al.[9] use dental images and voice. Kouno et al.[5] use a depth image from an overhead camera. Bednarik et al.[3] use gaze information such as pupil size, variation, gaze velocity, and distance of the infrared reflection of the eye. Nogueira et al.[12] use convolutional neural networks (CNN) for fingerprint authentication.

For behavioral characteristics, the authors have proposed an authentication method for a smartphone user from acceleration sensor data when taking it out of the pocket[6]. Guerra-Casanova et al.[7] proposed a method using gestures of their hands using a

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/1122445.1122456

mobile device with an embedded accelerometer. For motion-based authentication using accelerometers, acceleration characteristics of the motion until the helmet is worn can be used for authentication by mounting an accelerometer on the helmet. However, there are various wearing actions, such as wearing the helmet in a hurry and taking care not to let the interior of the helmet get wet in the rain. Therefore, it is not practical to collect data from all the people in various situations.

In this paper, we propose a method to identify individuals by acquiring their head shape while wearing a helmet with pressure sensors. Our method does not force the users to do special behavior, remain stationary, face to a camera, scan body identifier for identification. To breach our system, the exact three-dimensional shape of the head is needed, but it is difficult to replicate the head shape.

2.2 Head State Recognition

Toth et al.[15] focused on the facial muscle signal, and six different facial expressions were classified using the muscle signals and the gyroscope values obtained from a cheap off-the-shelf electroencephalogram (EEG) headset. EEG headsets are actually used to measure brain waves, however, the muscle signals are detected locally by placing electrodes on the scalp. Kwon et al.[10] designed a glass-type wearable device to detect the user's emotions based on facial expressions with a built-in camera and physiological reactions with photoplethysmogram (PPG) and electrodermal activity (EDA). Fukumoto et al.[8] designed a smile-based life-logging system that focuses on smile and laughter for indexing the interesting and enjoyable events on a recorded video. They use photo-interrupters. These researches obtain dynamic information such as facial expressions and physical responses in the face area. On the other hand, our study obtains static features of the head shape.

3 PROPOSED METHOD

This section describes the details of the proposed method.

3.1 Overview

The proposed method assumes that the user wears a helmet equipped with pressure sensors, acquires the shape of the wearer's head, and identifies whether the wearer is a registered person or not. The proposed method has two functions: user identification and user authentication.

User identification assumes that a single helmet is shared by multiple people and any other information such as ID is not given to the system. Their pressure sensor data are registered in advance and the person who put on the helmet is identified as one of the registered persons. User identification does not assume that a non-registered person will wear the helmet. If a non-registered person wears the device, the identification result will be the one with the closest data among the registered users.

User authentication determines whether the person wearing the helmet is actually the person or not when his/her ID or username is given. We assume two cases where the authentication is used: each individual has own helmet and only the person's pressure sensor data has been registered (single user; username preset in the device; the same as for smartphone authentication); and a helmet is shared with multiple people and username is entered

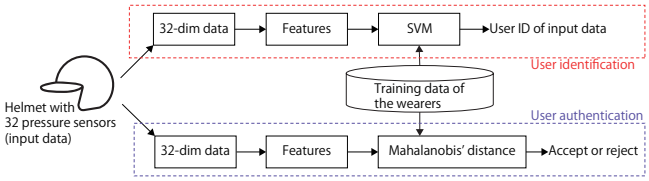

Figure 1: Flow of the user identification and authentication.

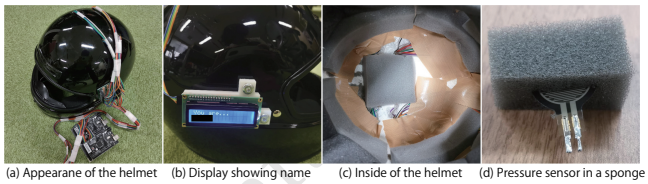

Figure 2: Prototype helmet with 32 pressure sensors.

when using the helmet (multiple users; username input accordingly; the same as for ATM authentication). Their pressure sensor data are registered in advance and the person who put on the helmet is judged to be accepted or rejected by calculating the similarity between the input data and the data of the ID. Even if an ID is leaked, an outsider can be rejected because his/her head shape is different from the data of the ID.

Figure 1 shows the flow of our system. 32 pressure sensors are attached to the inner side of the helmet to acquire data, producing 1-dimensional 32-channel pressure data sequence. Pressure data of the people who are expected to wear helmets have been registered to the system in advance and the data is called training data in this paper. In user identification, the system uses the support vector machine (SVM) to build a recognition model from the feature values extracted from the training data and outputs the identification results from the features of the input data of an unknown registrant. In user authentication, the system calculates Mahalanobis' distance between the training data and the input data of the person including non-registrant and authenticates the user if the distance is less than the threshold, otherwise the user is rejected.

3.2 Hardware

We implemented a helmet equipped with 32 pressure sensors as shown in **Figure 2**. We used a commercially available full-face helmet. The pressure sensors were FSR402 and FSR402 ShortTail manufactured by Interlink Electronics, Inc. The Arduino MEGA2560 R3 was used as a microcomputer. We installed a thick urethane sponge and inserted sensors into the cut line of the sponge. Four pressure sensors were set at the top of the head, 16 sensors were set around the top of the head, six sensors were set at the back of the head, and six sensors were set at the cheek pads on both sides as shown in **Figure 3**. The wiring for the pressure sensors went through a hole drilled in the top of the helmet. The PCB is bolted to the left cheek area using a threaded hole drilled for securing the helmet shield. It is fixed and removable. A display to show ID is attached to the right cheek area.

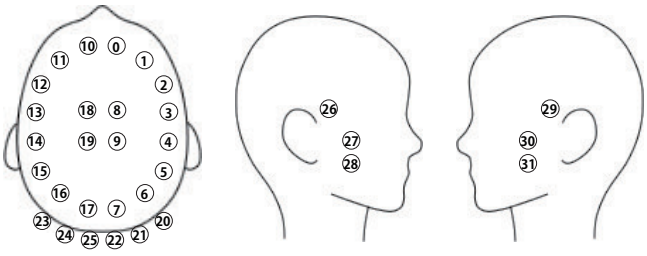

Figure 3: Positions of pressure sensors.

3.3 User Identification Method

3.3.1 Preprocessing. The data acquisition starts when the user puts on the helmet. 32 pressure sensors data $\boldsymbol{p}(t) = [p_1(t), \cdots, p_{32}(t)]$ is acquired at time t. The voltage values of all the pressure sensors are almost 5V when the helmet is not worn, showing sum of the data $\sum_{i=1}^{32} p_i(t) \approx 160[\mathrm{V}]$. When the helmet is worn, $p_i(t)$ decreases, and the system segments the data over 2-second window starting from the $t = T_s$ after the values are stabilized. Time $t = T_s$ is the time when the change of the sum of 32 dimensions per sample is first less than 2V for 11 consecutive samples (≈11/30 second as sampling rate is approximately 30 Hz) after the sum of 32 dimensions is less than 155V, i.e. $\sum_{i=1}^{32} |p_i(t) - p_i(t-1)| < 2[V]$ $(i = T_s, \cdots, T_s - 10)$. The average value over the window $x_i(t) = \frac{1}{N} \sum_{t=T_S}^{T_S+N-1} p_i(t)$ for sensor channel i $(i = 1, \cdots, 32)$ is calculated, where N is the number of samples in the window. We then obtain a 32-dimensional vector $\boldsymbol{x}(t) = [x_1(t), \cdots, p_{32}(t)]$ as a feature. Once the data is segmented, the preprocessing is suspended until $\sum_{i=1}^{32} p_i(t) > 159[\mathrm{V}]$ is met.

3.3.2 Identification. Given training data $[\boldsymbol{x}_m, y_m]$ $(m = 1, \cdots, M)$ from the users who are expected to use the helmet by wearing the helmet M times in total in advance, the SVM is trained with the training data, where y_m is the registrant label such as ID. The input data $\boldsymbol{x}_{test}$ collected by the user to be identified is fed into the SVM and the classification result $\hat{y}_{test}$ is obtained.

3.4 User Authentication Method

3.4.1 Preprocessing. In user authentication, 32-dimension pressure sensors data $\boldsymbol{p}(t) = [p_1(t), \cdots, p_{32}(t)]$ and its average $\boldsymbol{x}(t) = [x_1(t), \cdots, p_{32}(t)]$ as a feature are obtained in the same manner as in the user identification.

3.4.2 Similarity calculation. In user authentication, there are two cases of training data usage: data of a single user is used and data of multiple users is used. For single user data, data of only a single user, e.g., owner of the helmet, is registered or data of multiple users are registered but data of one of them whose ID is given is used. For multiple user data, data of multiple users who are expected to use the helmet is used. Given training data $[\boldsymbol{x}_m, y_m]$ $(m = 1, \cdots, M)$ from the user(s) by wearing the helmet M times in advance, the proposed method calculates the Mahalanobis distance, where y_m is the registrant label such as ID.

The Mahalanobis distance is one of the methods for calculating the distance between multiple variables, which can be normalized considering the distribution of the data. The mean vector $\boldsymbol{\mu} = \frac{1}{M} \sum_{m=1}^{M} \boldsymbol{x}_m$ and the variance-covariance matrix $\Sigma = \frac{1}{M} \sum_{m=1}^{M} (\boldsymbol{x}_i - \boldsymbol{\mu})(\boldsymbol{x}_j - \boldsymbol{\mu})^T$ of the training data are calculated. The Mahalanobis distance between training data $\boldsymbol{x}_m$ $(m = 1, \ldots, M)$ and input data $\boldsymbol{x}_{test}$ can be calculated with $d(\boldsymbol{x}_{test}, \boldsymbol{x}_m) = \sqrt{(\boldsymbol{x}_{test} - \boldsymbol{x}_m)^T \Sigma^{-1} (\boldsymbol{x}_{test} - \boldsymbol{x}_m)}$. If the test data are collected from the registered user, $\boldsymbol{x}_{test}$ follows the probability distribution of the variance-covariance matrix Σ.

3.4.3 Authentication decision. Let θ be the threshold value, the user is authenticated if $\theta \geq \min_m d(\boldsymbol{x}_{input}, \boldsymbol{x}_m)$ $(m = 1, \cdots, M)$ is satisfied, otherwise the the user is rejected.

4 EVALUATION

This section describes the experiments we conducted to evaluate the effectiveness of the proposed method.

4.1 Data Collection

We asked nine subjects (A–I, all males, mean age 23 years) to wear the helmet implemented in Section 3.2 and collected sensor data. The sampling rate is approximately 30 Hz. The subjects put it on for two seconds to collect data, then put it off, and put it on again for two seconds to collect data, through which a set of two samples is obtained. By collecting data of ten sets (20 samples) from each subject, a total of 180 samples (2 seconds×20 samples×9 subjects) were collected. Up to four sets of data were collected per person per day. In order to collect data on the various positions of the sensors and head as the helmet was worn, at least 30-minute break was provided between sets.

4.2 User Identification Method

4.2.1 Evaluation environment. We evaluated the proposed method in five-fold cross-validation manner that 80% (16 samples) of data collected from each subject were trained and 20% (four samples) were tested. In order to investigate the effect of the number of sensors used, identification accuracies for all combinations of sensors from one sensor to 32 sensors were measured. To simulate a half helmet which is commonly used at a construction site, we also tested with all combinations of 20 sensors aligned in the top half out of 32 sensors; #0–#19 in **Figure 3**. In this evaluation, two types of sensor configurations are tested: a full-face helmet with 32 sensors and a half helmet when 20 sensors.

4.2.2 Results and discussion. The accuracy of user identification with a full-face helmets and a half helmet is shown in **Table 1** and **Table 2**, respectively. The numbers shown in "Sensors used" are the sensor numbers in **Figure 3**. We found that all the accuracies when 32 and 31 sensors for full-face helmet are used and 20 and 19 sensors for half helmet are used were all 1.000. Therefore, we measured the accuracy from one sensor until the accuracy reaches to 1.000 and skipped the measurement of accuracies for more sensors. When the number of sensors is four, the number of sensor combination is ${}_{32}C_4 = 35960$, and the highest accuracy of 35960 combinations is shown in the table. For one through four sensors, the regularization parameter of SVM is set to $C = 1.0$, and the sensor combination with the highest accuracy was recorded. Then, the best C was searched by grid search for the sensor combination, and the highest accuracy is shown in the tables.

For full-face helmet, nine subjects were identified with 100% accuracy when the number of sensors was five. The accuracy was

Table 1: Identification accuracy with a full-face helmet; sensors are reduced from 32 to 1.

Sensors used	Accuracy
32 sensors	1.000
31 sensors	1.000
⋮	⋮
5 sensors	1.000
#0, #3, #5, #16	0.994
#3, #11, #24	0.972
#3, #25	0.922
#10	0.617

Table 2: Identification accuracy with a half helmet; sensors are reduced from 20 to 1.

Sensors used	Accuracy
20 sensors	1.000
19 sensors	1.000
⋮	⋮
5 sensors	1.000
#0, #3, #5, #16	0.994
#0, #3, #13	0.983
#3, #16	0.928
#10	0.617

Table 3: EER for the subjects in user authentication.

Subject	EER
A	0.002
B	0.095
C	0.050
D	0.055
E	0.006
F	0.094
G	0.012
H	0.050
I	0.000
Average	0.076

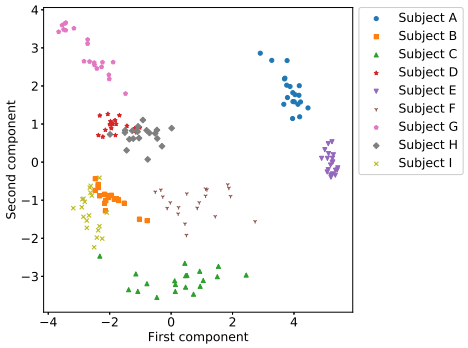

Table 4: 32-dimensional features compressed into two dimensions by PCA.

99.4% with four sensors, 97.2% with three sensors, and 92.2% with two sensors. However, the accuracy dropped significantly to 61.7% when the number of sensors was one. For half helmet, nine subjects were identified with 100% accuracy when the number of sensors was five. The accuracy was 99.4% with four sensors, 98.3% with three sensors, and 92.8% with two sensors. However, the accuracy dropped significantly to 61.7% when the number of sensors was one.

Focusing on the sensors used for full-face helmet, most of the sensors are less than #20, which means that sensors in the top half were significant. Sensors not used in half helmet were aligned around neck and ear and these sensor positions related to the user's head are supposed to be inconsistent.

4.3 User Authentication Method

4.3.1 Evaluation environment. One subject was considered to be the individual to be authenticated, i.e. owner, and the remaining eight subjects were considered to be strangers. The authentication accuracy of the owner was measured in five-fold cross-validation manner; 80% (16 samples) of the owner's data were registered as training data, and the remaining 20% (4 samples) data were used as test data. In addition, the rejection accuracy for the strangers were measured using data from all eight strangers (160 samples). All 160 samples were tested in each fold of the cross-validation. All nine subjects were evaluated on a rotation basis.

In user authentication, FAR (false acceptance rate), FRR (false rejection rate), and EER (equal error rate) are used as indicators of authentication accuracy. The smaller the threshold value θ is set, the stricter the authentication decision becomes, resulting in increasing FRR. There is a trade-off between FRR and FAR, and the value at which FRR equals FAR is called EER. Normally, the value of EER is used as an indicator to evaluate the performance of authentication methods, and smaller EER means better performance.

4.3.2 Results and discussion. EER of each subject and the average are shown in **Table 3**. EER of subjects A, E, G, I were roughly less than 0.01, which means that the owner fails in authentication less than once a 100 times, and that the strangers break the authentication less than once a 100 times. EER of 0.0097 for user authentication using ear acoustics was reported in Ref. [14], therefore, our method achieved comparable performance for four of nine subjects.

The next most accurate subjects are C, D, H, with EER of approximately 0.05. In order to determine the cause of the decline in accuracy compared with subject A, E, G, I, all collected data were compressed to the first and second principal component by principal component analysis (PCA). The results are shown in **Figure 4**. Looking at the plots of subject C, one sample of subject C is close to data of subject I and the variance in the first principal component is large, which would deteriorate the accuracy. On the other hand, the data for subjects D and H overlapped each other significantly, which affected the accuracy of the both subjects.

The least accurate subjects are B and F, with EER of approximately 0.095. From the figure, data of subject B has a small variance and there is some overlap with data of subject I. However, EER of subject I was 0, which is perfect authentication. Therefore, the overlap of these data groups would be due to the loss of data by PCA. On the other hand, data of subject F does not show any overlap with the other subjects' data, but there is a large variance to both directions for the first and second principal components. Considering the effect of data compression by PCA, duplication with other subjects' data groups can be inferred in the 32-dimensional data. The accuracy of subjects B and C, who has data located close to the data of subject F, may have been affected by the scattered data of subject F. In particular, the accuracy of subject B is lower than that of subject C because the two samples of subject B are located in close proximity to the data of subject F.

5 CONCLUSION

In this paper, we proposed a method to identify individuals based on individual differences in head shapes which is measured by wearing a helmet with pressure sensors. We implemented the prototype device with 32 pressure sensors and evaluated the proposed method with nine subjects. The results showed that 100% identification accuracy for nine subjects was achieved with five sensors. EER of four out of nine subjects showed less than 0.012, and the average EER was 0.076 in the authentication.

REFERENCES

[1] J. Ajay Siddharth, A. P. Hari Prabha, T. J. Srinivasan, and N. Lalithamani. 2017. Palm Print and Palm Vein Biometric Authentication System. In *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, Subhransu Sekhar Dash, K. Vijayakumar, Bijaya Ketan Panigrahi, and Swagatam Das (Eds.). Springer Singapore, Singapore, 539–545.

[2] R.G. Attewell, K. Glase, and M. McFadden. 2001. Bicycle helmet efficacy: a meta-analysis. *Accident Analysis & Prevention* 33, 3 (2001), 345–352. https://doi.org/10.1016/S0001-4575(00)00048-8

[3] R. Bednarik, T. Kinnunen, A. Mihaila, and P. Fränti. 2005. Eye-Movements as a Biometric. In *Image Analysis*, Heikki Kalviainen, Jussi Parkkinen, and Arto Kaarna (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 780–789.

[4] Y. Chen, J. Sun, X. Jin, T. Li, R. Zhang, and Y. Zhang. 2017. Your face your heart: Secure mobile face authentication with photoplethysmograms. In *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*. 1–9.

[5] D. Kouno, K. Shimada, and T. Endo. 2013. Person Identification Using Top-View Image with Depth Information. *International Journal of Software Innovation* 1, 2 (2013), 67–79.

[6] *****Blind for review*****. [n.d.].

[7] J. Guerra-Casanova, C. Sánchez-Ávila, G. Bailador, and A. de Santos Sierra. 2012. Authentication in mobile devices through hand gesture recognition. *International Journal of Information Security* 11, 2 (2012), 65–83. https://doi.org/10.1007/s10207-012-0154-9

[8] K. Fukumoto, T. Terada, and M. Tsukamoto. 2013. A smile/laughter recognition mechanism for smile-based life logging. In *Proceeding of of the 4th Augmented Human International Conference (AH '13)*. 213–220.

[9] D. Kim and K. Hong. 2008. Multimodal biometric authentication using teeth image and voice in mobile environment. *IEEE Transactions on Consumer Electronics* 54, 4 (2008), 1790–1797.

[10] J. Kwon, D. Kim, W. Park, and L. Kim. 2016. A wearable device for emotional recognition using facial expression and physiological response. In *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. 5765–5768.

[11] T. Nakao, N. T. Hung, M. Nagatoshi, and H. Morishita. 2012. Fundamental study on curved folded dipole antenna. In *Proceedings of the 2012 IEEE International Symposium on Antennas and Propagation*. 1–2.

[12] R. F. Nogueira, R. de Alencar Lotufo, and R. Campos Machado. 2016. Fingerprint Liveness Detection Using Convolutional Neural Networks. *IEEE Transactions on Information Forensics and Security* 11, 6 (2016), 1206–1213.

[13] A. Sayo, Y. Kajikawa, and M. Muneyasu. 2011. Biometrics authentication method using lip motion in utterance. In *2011 8th International Conference on Information, Communications Signal Processing*. 1–5.

[14] T. Arakawa, T. Koshinaka, S. Yano, H. Irisawa, R. Miyahara, and H. Imaoka. 2016. Fast and Accurate Personal Authentication using Ear Acoustics. In *2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*. 1–4.

[15] J. Toth and M. Arvaneh. 2017. Facial expression classification using EEG and gyroscope signals. In *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. 1018–1021.