Research on information security of users’ electricity data including electric vehicle based on elliptic curve encryption

Renwu Yan1, Chuan Lin2, Wen-feng Zhang3, Li-wen Chen3 and Kang-ning Peng3

Abstract
In the smart grid and big data environment, accurate and large amount of power load data for users can be obtained with the wide application of non-intrusive load monitoring technology. In the research process of customers’ information, information security protection of users’ electricity data has become a research hotspot urgently. This article proposes a new type of load decomposition method for electric vehicle load information and compares it with hidden Markov model algorithm to verify its accuracy. On this basis, the elliptic curve encryption algorithm is used to encrypt the users’ electricity data, and the function and effectiveness of the encryption algorithm are verified by comparing the load decomposition of the electric vehicle with the unencrypted data.

Keywords
Information security, electric vehicle, smart grid, elliptic curve cryptography algorithm, load decomposition

Date received: 4 June 2020; accepted: 24 September 2020

Handling Editor: Peio Lopez Iturri

Introduction
With the dramatic development of smart grid and electric vehicle, machine learning methods have been widely used for information security of smart grid in various fields1,2 such as non-intrusive load monitoring technology,3 information inference attack and preserving,4,5 and Internet of Things technology.6 On the aspect of researches on users’ electricity load identifications, it is mainly focused on the identifications of users’ load equipment.7–9 Yet, it is precisely in the smart grid and big data environment that users’ electricity data face serious information security threat. In the process of big data information being researched, the privacy protection of information is also a major problem to be solved.10–12 Previous studies13–15 proposed $k$-anonymity and its improved algorithm to generalize and compress the sensitive data to achieve the purpose with hidden
data. Wu et al.° proposed blind signature, anonymous processing, and Paillier homomorphic encryption to realize the anonymous data transmission and to protect users' electricity data from being leaked.

In this article, a new type of load decomposition is applied for the process of load decomposition, including electric vehicles' load signals, and compared with hidden Markov model (HMM) algorithm to prove its superiority. At the same time, the security of the users' electricity data is considered during the transmission. The feasibility of the ECC algorithm is verified by the decomposition results of encrypted and unencrypted data.

**New load decomposition algorithm**

The new load decomposition algorithm is a method of separating the electric vehicles' charging signals from the gathered house electrical power signals. This method can effectively alleviate the interference from household appliances except electric vehicles (especially from air-conditioning (AC) system). In this way, electric vehicles' charging signal detection and electric power estimation can be accurately realized under the interference from the power signals of AC system.

**New load decomposition algorithm implementation steps**

Threshold processing of aggregated signals. For a given aggregated signal, the threshold signal is first applied to the aggregated signal for threshold processing, the portions of which having an amplitude less than the specified threshold are deleted, and the waveforms greater than the threshold portions are retained. The following is the threshold processing formula

\[
x(t) = \begin{cases} 
x(t) & \text{if } x(t) \geq \Lambda \\
0 & \text{if } x(t) < \Lambda
\end{cases}
\]

(1)

here, \( \Lambda = \max \{2.5, \frac{1}{2|k|+2} \sum_{|k|+2} x(k)\} \), where \(|x(k)|>2|\) refers to the sampling numbers that are more than 2 kW and the symbol \( \Lambda \) represents equal by definition.

Filter AC pulse sequence. After the aggregated signal is processed by threshold, the AC pulse sequence still needs to be removed. Assuming that the duration of AC pulse sequence does not exceed minutes, the sequences that pulse sequences are not exceeding minutes are marked as "segments to be deleted." One of the "segments to be deleted" is taken as initial data, and the adjacent "to-be-deleted segments" are analyzed and checked whether it meets the following two conditions

\[
T_{\text{filter}} < D(1 + \eta)D_{\text{cur}}
\]

(2)

\[
G_{\text{ap}} \leq 3D_{\text{cur}}
\]

(3)

where \( T_{\text{filter}} \) indicates the duration of a "to-be-deleted segment" adjacent to the initial "deleted segment," \( D_{\text{cur}} \) indicates the duration of the initial "deleted segment," \( \eta \) represents the duration extension parameter, \( D \) is defined as the parameter value with the influence of \( D_{\text{cur}} \) and \( \eta \), and \( G_{\text{ap}} \) indicates the distance between the initial "to-be-deleted segment" and the adjacent "to-be-deleted segment."

The adjacent "to-be-deleted segment" that satisfies the above two conditions will be marked as a new initial "to-be-deleted segment." The above filter operation is repeated again. If the search criteria do not meet the above requirements of the filter, then the next pulse sequence segment will be initially checked. All periods of time marked as "segments to be deleted" are deleted from \( x(t) \) until the search for the entire aggregated signal is completed. In order to prevent from accidentally deleting a waveform segment with a long duration (this waveform segment generally is a power signal containing electric appliance such as electric cars, dryers, and ovens), a threshold time \( T_1 \) can be set so that the duration of all deleted segments does not exceed the specified threshold \( T_1 \).

**Removal of residual interference.** There are many residual interference in the aggregated signal, which refer to the fluctuations in the power signals of electrical appliances, the loss of the power line, and the hybrid error of low-amplitude electrical appliances' power signals. After the threshold processing, the position information of each divided waveform segment can be obtained, and the residual interference amplitude around each segment can be estimated. The amplitude of the interference of each segment is estimated by taking the average value between the minimum value before segmentation of point A and the minimum value after segmentation of point B.

For each waveform segment, we can set two reference points to distinguish them. The minimum value of A is set as a reference before each segment, and the minimum value of B is set as a reference point after each segment. We can estimate the interference amplitude of each segment by averaging the minimum values of these two reference points. The residual interference amplitude can be removed by subtracting the segment from other related local interference.

**Classification of segmented signals.** After the above processing, the resulting aggregated signal leaves only a
few signals which can be divided into the following three categories.

First, the cumulative counting function is defined

\[ f(r) = \langle H(t) > r \rangle \]  

where \( H(t) \) represents the aggregated signals after the first three steps of processing and \( r \) represents a threshold value of maximum amplitude value from 0 to \( H(t) \). The function of equation \( H(t) > r \) is to calculate the sampling points whose amplitude values are greater than \( r \) in \( H(t) \).

Second, the gradient function \( g(r) \) of the cumulative function \( f(r) \) is calculated, and the type of the segmented signal can be initially judged based on the number of peaks of the gradient function. The segmented signal belongs to the third type when two gradient peaks appear in the gradient function. The segmented signal belongs to the second type when the gradient function exhibits a prominent peak. The segmented signal in the first type does not show a prominent peak.

Third, a normalized gradient function is defined if the gradient function has two segmented signals above two prominent peaks

\[ gn = g / \max(g) \]  

Then, calculate the areas, \( S_n \) and \( S_q \), under the curve \( g_n \). If

\[ S_q > 35\% S_d \]  

And the segmented waveform is classified as the first type of waveform; otherwise, it is classified as the third type of waveform.

Reconstruction of various types of electric vehicle charging load waveform. After classifying the segmented waveform in the first four steps, it is necessary to take one more step to extract the electric vehicle charging load waveform in the sub-class of Figure 1. The effective width \( W_{valid} \) of each waveform segment is hereby defined as the width (time) at the bottom of this waveform segment. However, the effective height \( H_{valid} \) is defined as the height when the waveform segment width is only 80% of the bottom width.

Neutron class identification of three types and the processing of electric vehicle charging load waveform reconstruction are shown in Figure 2.

When the electric vehicle charging load overlaps with other equipment loads, the electric vehicle charging load waveform needs to be restructured. Considering that the electric vehicle waveform has a characteristic of constancy and amplitude stability, the height of the electric vehicle waveform can be estimated on the same day or some other time in a single day. Therefore, this article uses the actual height of the electric vehicle charging load and calculates the effective width of the segmented signal to reconstruct the square waveform of the electric vehicle.

Evaluation index for new load decomposition algorithm effect

In order to evaluate the efficacy of the decomposition algorithm, three evaluation indicators are defined, as follows:

1. Average estimated error percentage \( ER_1 \) of monthly electricity usage

![Figure 1. Three types of segmentation signals.](image-url)
Average estimated error of monthly electricity consumption

$$ER_1 = \frac{1}{N} \sum_i \sum_j \left( \frac{|E_i^{i,j} - E_e^{i,j}|}{E_i^{i,j}} \right) \times 100\%$$  \hspace{1cm} (7)

2. Average estimated error $ER_2$ of monthly electricity consumption

$$ER_2 = \frac{1}{N} \sum_i \sum_j \left( \frac{|E_i^{i,j} - E_e^{i,j}|}{E_i^{i,j}} \right) \text{(kW \cdot h)}$$  \hspace{1cm} (8)

3. Mean square error ($MSE$) of electric vehicle charging load signals

$$MSE = \frac{1}{N} \sum_i \sum_j \left( \frac{(E_i^{i,j} - E_e^{i,j})^2}{(E_i^{i,j})^2} \right) \times 100\%$$  \hspace{1cm} (9)

where $E_i^{i,j}$ indicates the actual charging loads of the electric vehicle in the $j$th month of the $i$th year, $E_e^{i,j}$ indicates the estimated charging loads of the electric vehicle in the $j$th month of the $i$th year, and $N$ is the total months.

**ECC algorithm**

ECC algorithm is an asymmetric cryptosystem based on the elliptic curve discrete logarithm problem. It has strong unit data security and it is widely used due to the advantage of its short key. Based on the finite field arithmetic operation, ECC algorithm is easy to complete using computer operation.\(^{17,18}\)

**Prime field elliptic curve**

Set $p$ as a prime number, and the entire remainder set \(\{0, 1, \ldots, (p - 1)\}\) of modulo $p$ with respect to modulo $p$ constitutes a finite field $F_p$ of a $p$-order prime number. Prime field $F_p$ can define an elliptic curve

$$y^2 = x^3 + ax + b \text{ (mod } p)$$  \hspace{1cm} (10)

where $a, b \in F_p$, $(4a^3 + 27b^2) \text{ mod } (p) \neq 0, x, y \in F_p$.

The pair $(x, y)$ is a point on formula (10), and an infinity point $\infty$ of additional regulation is also a point on equation (10). In that way, the set $E_p(F_p)$ of points on the curve determined by the elliptic curve in equation (10) on the prime field $F_p$ is

$$E_p(F_p) = \{ (x, y) \in F_p \cup \infty \}$$  \hspace{1cm} (11)

If there is a point $P$ on the elliptic curve and there exists a minimum positive integer $n'$, which make multiplication $n'P = O_\infty$, then $n'$ will be called as the order of $P$, and if $n'$ does not exist, then $P$ is of infinite order.

**ECC encryption and decryption principle**

An elliptic curve on $F_p$ is usually described as $Tm = (p, a, b, G, n, h)$. An elliptic curve can be determined by $p$, $a$, and $b$; the base point is $G$; the order of point $G$ is $n$; $m$ represents the number of all points on the elliptic curve; and $h$ is the integer part of a quotient of $m/n$. Take the electric power user DJ using elliptic curve encryption to send the household load information in plain text $X$ to the electric power company DM as an example.\(^{19,20}\) The design flow is shown in Figure 3.
Case analysis

This section is based on the aggregated power signal data from Hickory Street Database of the Americas someday. Through the new load decomposition algorithm mentioned above, the process of decomposing the charging load waveform of the electric vehicle for 1 day is described in detail and compared with the HMM method proposed in Zheng et al.21 The accuracy is verified.

Implementation of new load decomposition algorithm

Threshold processing of aggregated signals. The threshold $\lambda = 2500$ is set. The effect of the initial threshold processing of the aggregated power signal of a certain day, according to formula (1), is shown in Figure 4.

By comparing the aggregated signals after the threshold processing with the signals before the threshold processing, the bottom burr waveform is sharpened and appears flat.

Filter AC pulse sequence. It can be seen from the aggregated signal after the threshold processing that there are still many AC pulse sequences in the signal which need to be filtered out.

Set the parameters $T = 10$, $\eta = 1$, $T_1 = 90$, and set the filter according to formula (2), formula (3), and $T_1$ anti-false filter parameters. The filtering effect is shown in Figure 5.

After filtering the AC pulse sequence, the aggregated signal has retained several segmented waveforms (there are two segmented waveforms in Figure 4). The filtering effect is significant.

Removal of residual interference. Set the position of $A = 5$ and $B = 5$ as reference points and remove the interference amplitude using the above methods of removing residual interference. The effect after removing the residual interference is shown in Figure 6.

After that, the signal for removing the residual interference can redo the threshold process and filter the AC pulse sequence process. Now move to the next step.

Classification of segmented signals. As it can be seen from Figure 5, the remaining two segmented waveforms need...
to be classified after the threshold process and filtering process.

According to equation (4), the cumulative counting functions, $f_1(r)$ and $f_2(r)$, corresponding to the two segmented waveforms, $x_1(t)$ and $x_2(t)$, and their corresponding gradient functions, $g_1(r)$ and $g_2(r)$, are solved. The curves are shown in Figures 7 and 8, respectively.

It can be seen from waveform $g_1(r)$ of Figure 7 that there is a peak value. For this reason, this segment can be classified as the second type. There are two peak values that can be seen from waveform $g_2(r)$ of Figure 8. Accordingly, this segment can be classified as the third type. Convert $g_2$ of Figure 7 to a standardized gradient function based on equation (5) and calculate
Sn = 30.65% × S_n < 35%S_q based on equation (6). In the same way, the second segment can be judged as the third type.

Reconstruction of various types of electric vehicle charging load waveform. The segmented waveform of Figure 7 is the second type of waveform. Hence, the effective height $H_{\text{valid}}$ and the effective width $W_{\text{valid}}$ of the waveform of Figure 9 are calculated first.

The segmented waveform of Figure 9 is the third type of waveform. First, determine whether the electric vehicle charging load waveform is on the top or bottom of the segmented waveform.

Set the threshold $\lambda_2 = \lambda + 3000 = 5500$, and the effective time width calculated is 257 min, less than 300 min. Consequently, the sub-segment waveform needs to be analyzed in the next step. Figure 10 is a sub-segment waveform where the segmented waveform is filtered again. Figure 11 is a waveform where the segmented sub-segment waveform is subjected to a capacity filling process.

The filtering does not delete the sub-segment waveform. Therefore, the top of the sub-segment waveform is the electric vehicle charging load. Then, the effective height and effective width of the top of the sub-segment waveform in Figure 11 are also obtained using the way shown in Figure 9. Eventually, the electric vehicle charging load waveform in the aggregated signal is reconstructed, as shown in Figure 12.

Based on the aggregated signal, three decomposition effect evaluation indexes are calculated respectively.
based on equations (7)–(9): $ER_1 = 10.2$, $ER_2 = 1.203$ (kW · h), and $MSE = 0.02$ can be concluded.

**Comparisons between new load decomposition algorithm and HMM algorithm**

The new load decomposition algorithm proposed in this article and the HMM algorithm proposed in Zeadally et al. are used under the same conditions. Users’ electric vehicle load waveforms of Hickory Street Database of the Americas are decomposed. The data in Table 1 can be obtained.

As shown in Table 1, the average estimated errors of monthly electricity consumption are compared. The errors of the new algorithm are smaller than the errors of the HMM algorithm. As for the average estimation error of electric energy consumption of 8.44% of the new algorithm, the estimation error of HMM algorithm which is up to 64.4% is undoubtedly not suitable for energy decomposition with electric vehicle charging signals. Therefore, the new algorithm is better than the HMM algorithm.

**ECC-based encrypted signal decomposition**

The ECC algorithm is used to encrypt the aggregated signal of a certain day. Parameter setting of ECC algorithm is calculated as follows:

1. $y^2 = x^3 + ax + b \pmod{p}$ in equation (10) is selected as the encrypted elliptic curve;
2. With regard to the determination of parameter $p$, the larger the $p$-value, the safer it will be. But
it will also affect the calculation speed. In order to meet the security requirements, a prime number of about 200 bits is generally selected;

With regard to the determination of parameters $a$ and $b$, $a$ can be a positive integer randomly generated which is less than $p - 1$. After the determination of $a$ depending on the condition in equation (13), we have

$$a, b \in F_p, (4a^3 + 27b^2) \mod (p) \neq 0$$ (12)

A positive integer $b$ less than $p - 1$ is randomly generated again.

4. About the determination of the base point, the determination of curve $y^2 = x^3 + ax + b (\mod p)$ is based on the determination of parameters $a$, $b$, and $p$. The $x$ coordinate of the base point $G$ can be an arbitrary integer from 0 to $p - 1$. When the $x$ coordinate of the base point $G$ is determined, the $y$ coordinate of the base point $G$ can be obtained by the inverse operation of $y^2 = x^3 + ax + b (\mod p)$;

5. For the determination of the private key $k$, randomly select a prime number from 0 to $p - 1$ as the private key $k$;

6. With regard to the determination of the public key $K$, multiply $k$ by the base point $G$ to get the public key $K$, which is $K = kG$.

The process of decomposing the charging load waveform of the electric vehicle is described as shown above. After that, stealers can only obtain the encrypted signal as shown in Figure 13 at most. Compared with the encrypted signals and unencrypted signals, the encrypted one expands to an order of magnitude with violent vibration frequency. Afterwards, the new decomposition algorithm is used to decompose the encrypted signal to verify whether it can also decompose the electric vehicle load waveform or not and prove its encryption security. The decomposition results are shown in Figure 14.

As it can be seen from Figure 14, the load waveform of the electric vehicle with the signals encrypted cannot be decomposed by the new decomposition method, which ensures the security of signals during the transmission.

| User | $ER_1$ (new) | $ER_2$ (new) | MSE (new) | $ER_1$ (HMM) | $ER_2$ (HMM) | MSE (HMM) |
|------|--------------|--------------|-----------|--------------|--------------|-----------|
| 1    | 8.0%         | 11.7         | 0.31      | 133.5%       | 192.2        | 1.51      |
| 2    | 9.6%         | 20.3         | 0.30      | 26.0%        | 58.0         | 0.47      |
| 3    | 7.0%         | 12.3         | 0.27      | 38.8%        | 73.1         | 0.46      |
| 4    | 11.7%        | 24.5         | 0.29      | 76.2%        | 156.5        | 0.96      |
| 5    | 5.9%         | 9.9          | 0.16      | 47.6%        | 81.3         | 0.63      |
| Average | 8.44%         | 15.74        | 0.26      | 64.4%        | 112.2        | 0.8       |

HMM: hidden Markov model; MSE: mean square error.

Figure 13. Unencrypted signal (top) and encrypted signal (bottom).
Conclusion

This article proposes a new type of load decomposition algorithm especially for electric vehicle users. By comparing with the HMM algorithm, the superiority of the new load decomposition algorithm is verified from three evaluation indicators, $ER_1, ER_2, MSE$. Based on this, an ECC-based data encryption scheme is put forward and the proposed new load decomposition algorithm is applied to decompose the encrypted user power aggregation signal. The experimental result shows that the new load decomposition algorithm cannot decompose the electric vehicle load waveform in the encrypted aggregate signal, verifying the security on the basis of ECC data encryption scheme. In the future, a growing number of terminals will communicate with electric vehicles.25–28 Researches in the field of data security and privacy protection will be increasingly emphasized. This article will find other ways of data aggregation encryption for further exploration and propose communication encryption for owners of electric vehicles.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was supported by the Natural Science Foundation of Fujian Province of China (Grant Nos 2018H0003, 2017J01731, and 2017J01732) and Educational Commission of Fujian Province of China (Grant Nos JT180339 and JAT171096).

References

1. Cai Z, Zheng X and Yu J. A differential-private framework for urban traffic flows estimation via taxi companies. *IEEE T Ind Inform* 2019; 15(12): 6492–6499.
2. Wang J, Cai Z and Yu J. Achieving personalized k-anonymity based content privacy for autonomous vehicles in CPS. *IEEE T Ind Inform* 2020; 16(6): 4242–4251.
3. Yang J, Zhao J, Wen F, et al. Residential appliance identification and load modeling based on big data mining in smart grid environment. *Electr Power Constr* 2016; 37(12): 11–23.
4. Zeng N, Wang Z, Zhang H, et al. An improved particle filter with a novel hybrid proposal distribution for quantitative analysis of gold immunochromatographic strips. *IEEE T Nanotech* 2019; 18(1): 819–829.
5. Cai Z, He G, Guan X, et al. Collective data-sanitization for preventing sensitive information inference attacks in social networks. *IEEE T Depend Secur Comput* 2018; 15(4): 577–590.
6. Zhang L, Cai Z and Wang X. FakeMask: a novel privacy preserving approach for smartphones. *IEEE T New Service Manag* 2016; 13(2): 335–348.
7. Wu X and Wang Z. A non-intrusive decomposition algorithm for resident power load based on negative entropy estimation. *Power Syst Technol* 2017; 41(3): 932–937.
8. Sun Y, Cui C, Lu J, et al. Non-intrusive load monitoring method based on delta feature extraction and fuzzy clustering. *Autom Electr Power Syst* 2017; 41(4): 86–91.
9. Chen S, Gao F, Liu T, et al. Load disaggregation method based on factorial hidden Markov model and its sensitivity analysis. *Autom Electr Power Syst* 2016; 40(21): 128–136.
10. Wang D, Yuan J and Shen Z. Interactive queries differential privacy protection model in big data environment. *Appl Res Comput* 2019; 36(6): 116–121.

ORCID iD

Renwu Yan https://orcid.org/0000-0003-3531-5400
11. Xiong X, Liu S, Li D, et al. Private electric vehicle charging location aggregation based on local differential privacy. *Adv Eng Sci* 2019; 51(2): 137–142.

12. Liang Y, Cai Z, Yu J, et al. Deep learning based inference of private information using embedded sensors in Smart devices. *IEEE Netw Mag* 2018; 32(4): 8–14.

13. Abidi B and Yahia SB. Generating k-anonymous micro-data by fuzzy possibilistic clustering. In: *Proceedings of international conference on database and expert systems applications*, Lyon, 28–31 August 2017, pp.3–17. New York: Springer.

14. Mezher AM, Alvarez AG, Rebollo-Monedero D, et al. Computational improvements in parallelized k-anonymous microaggregation of large databases. In: *Proceedings of the IEEE, international conference on distributed computing systems*, Atlanta, GA, 5–8 June 2017, pp.258–264. New York: IEEE.

15. Dargahi T, Ambrosin M, Conti M, et al. ABAKA: a novel attribute-based k-anonymous collaborative solution for LBSs. *Comput Commun* 2016; 85: 1–13.

16. Wu Y, Lv WL, i C, et al. Smart meter data privacy protection scheme based on authentication and aggregation encryption. *J Northeast Elect Power Univ* 2018; 35(5): 91–96.

17. Zhang X, Tong W, Wang T, et al. Cipher texts generation method in elliptic curve cryptography based on plaintext length. *J Comput Appl* 2015; 35(10): 2863–2866.

18. Liu Y, Lang X and Pei SJ. An lightweight elliptic curve cryptography for terminal small devices. *Sci Tech Eng* 2019; 19(2): 131–134.

19. Daniel S, Robert L and Oldham NJ. Optimization of elliptic curve operations for ECM using double & add algorithm. In: *Forth international conference on e-technologies and networks for development (ICeND)*, Lodz, 21–23 September 2015, pp.1–4. New York: IEEE.

20. Sen N. An efficient ID based security algorithm for mutual node authentication and key management: an elliptic curve cryptography based approach. *Appl Algorithm* 2014; 8321: 110–121.

21. Zheng X, Cai Z and Li Y. Data linkage in smart IoT systems: a consideration from privacy perspective. *IEEE Commun Mag* 2018; 56(9): 55–61.

22. Zeadally S, Pathan ASK, Alcaraz C, et al. Towards privacy protection in smart grid. *Wirel Pers Commun* 2013; 73(1): 23–50.

23. Diao F and Zhang FG. Full privacy preserving smart metering system. *J Cryptologic Res* 2014(4): 400–409.

24. Xiong Z, Li W, Han Q, et al. Privacy-preserving auto-driving: a GAN-based approach to protect vehicular camera data. In: *19th IEEE international conference on data mining (ICDM)*, Beijing, China, 8–11 November 2019. New York: IEEE.

25. Liang T, Li Y, Shi C, et al. Design and implementation of information security gateway for electric vehicle. *Comput Appl Softw* 2017; 34(3): 277–283.

26. Liu Shui, Cai Wen, Zhou Qi, et al. Smart charging management system of electric vehicle based on wireless communication technology. *Elect Meas Instrum* 2018; 55(S1): 90–93.

27. LeCun Y, Bengio Y and Hinton G. Deep learning. *Nature* 2015; 521: 436–444.

28. Zeng N, Zhang H, Song B, et al. Facial expression recognition via learning deep sparse autoencoders. *Neurocomputing* 2018; 273: 643–649.