100%

Despite neural network-based speaker recognition systems (SRS) have enjoyed signi ficant success, they are proved to be quite vulnerable to adversarial examples. In practice, the SRS model parameters are not always available. Attackers have to probe the model only via querying, and such decision-based attacking merely relies on the output label is quite challenging. This letter proposes a two-step query-efficient decision-based attack based on local low-frequency perturbation. Specifically, instead of imposing perturbation on the entire audio sample, a local attacking region is firstly sought, confining the perturbed distortion to a local region. Second, considering that the majority of energy concentrates on the low-frequency bands, the proposed method suggests performing perturbation generation in the low-frequency domain. Experimental results demonstrate that, compared with the recent methods, our method could implement target attacking to SRS with a higher attacking success rate, at the cost of much lower queries and adversarial perturbation.

参数设置

60%

Despite neural network-based geaker recognition systems (SES) have enjoyed signit Scant success, they are proved to be quit wo tulnerable to detwarmid complex in practice, they are proved to be quit wo tulnerable to detwarmid complex in practice, they are proved to the control to the con

50%

segion nemal necessivants appaire recognition presses DBD have suppost significant scanners. He describes that describes the describes the describes that describes the describes the practice, the dBD model parameter are not always excitable, detection and provide the model of privile querying, and such describes describes are stated provided and the supposition of the sup

40%

In particular thresholds and special as related for the control fluctuations. The control is related to the control in the present to be equivalent to a demand on the present to the control in the cont

Results of Tencent OCR

Images

Persists must, inwinely-based papeler recognition critical (IEEE) have explored significant masses, there are arrest to be usin values files as showed all significants assessed, and the same of the significant files and the significant files and the significant files and the significant files all significant files all significant files all significants and stated using the significant files all significant signif

中華文庫会 中華文庫会 ・

Despite neuralineterisk-based speakenrecognition
systemic/REJ lava enjoyed sigit

heart success, they are proved to be quite vulnerable to a

cheverantil example.

In practice, the SRS model parameters are not always
available, Andorsen have

to prefe the model only via quarying, and such decision-based

attacking menyl

relies on the output field in quite challengins. This letter
proposes a to-ceilar

query-effhcient decision-bssed attack based on locallow-

全文还原 印制指用 json语图₀

frequency perturbation

Despite search service based grander recognition protons (IRI) have a gived size faster transet, there expressed to be utilized by a behavioral and reference and the search of the sear

PSREE

中華文庫

Despite nouralinstanch. Assert speakeneocognition systems(ARI) have enjoyed sign!
hard success, they are preed to be quite vulnerable to aniversarial examples.
In praction, the SRS mode parameters are not always available. Altadens have a price her need only vis querying, and such decision-based altadaring memby

seles on the output label in quite challengine. This letter proposes is to-olisip
query-efficient decision-based altada based on localisos-





Results of Alibaba OCR

Despite neural network-hand quesker recognition systems (MES) have enjoyed similated moreaus, they are proved to be quite valuareable to adversarial consultation moreaus, they are proved to be quite valuareable to adversarial consultation to provide the solid quite qualitation and moderation-shead statistics provide relieve on the enters index continues and tenderation for local per-frequency perturbations. Specifically, instead of impossing perturbation on the enters and/or amplitation of the enters amplitation of the ente

The control was designed under your tracking the law of the control TW. The control make that counts, there is seen of the justice classifies to designed under the control make. The control was the control

promote by the gainst value of international transitions, and promote, the SS from deligible promoters are not always statistical Austrant have a to profit the model only on a statistical Austrant have a to profit the model only on a statistical Austrant have a top of the statistic sta

全文正理 学别结果 json语目_®





全文正展 FRMAR Non表出点



De gal two on and inclusión based que les mongations appeten mobilità here projectif a li le net to cor a altre per possibilità del projectif a li le net to cor a altre per possibilità del projectif del projectif

全文正数 PRIMEM joonEEEg







