????
?
???????
???????
?
?32 × 32299 × 299
$m \times nm' \times n$??
$_s caling.png$Concept$Demonstratingtheconceptofimagedownscaling.$Source$Thepixels_{11}Q_{12}Q_{21}Q_{22}P$[?].
?
?
?
?
~~a)b)?~~
?
??fast gradient sign method
??????[1]
??????[2]
?
?
??
?
?
?
??[3]
$_a ttack_s ymbols.png$Showingthemajorobjectsofanimage − scalingattack?.

$_s cale_c oncept.png$Demonstratingtheconceptofanimage − scalingattack?.
?
a)b)?
$AA\Delta_1 SA = S + \Delta_1$??$Ascale()A_i AO_1O_2$??$TO_1\Delta_2 ASTL$?$A$

N_{max}
$Iscale(I) = L * I * RLRm' \times mn \times n'm \times nILR$

?
??I
$IIII'$??
?
$\beta II'\sigma I\beta\sigma\beta_h\beta_v\sigma_h\sigma_v\beta\sigma\sigma\beta\beta\sigma$
IO_1O_2??
?IAI'
$nnn = 2568I$
8256
?
$S'SA$
Selective Median Filter:$A2\beta_h * 2\beta_v$
Selective Random Filter:
??$\beta\sigma\sigma\beta\sigma\sigma\beta$
?
???$XAX = S + \Delta\Delta S$
A^4
?
????
$ST'SSTA$
??
??
???$D_rD_aD_rD_aD_aD_a$??
O_1O_2??$O_1scale(S)Tscale(S)TO_1O_2 \geq O_2SA$
$\beta\sigma$??$\sigma\sigma O_2 \geq$?O_1??O_2??σ?
O_1?
O_2?
O_1
?
??
???$256 \times 25632 \times 32$
???
?
??$Ascale(A)Ascale(A)$
O_1O_2
~~a)~~
a) ~~b)~~
b) ~~c)~~
c)
??
Image-Scaling Attack without defense:$O_1DT > O_2O_2$

a)b)c)b)