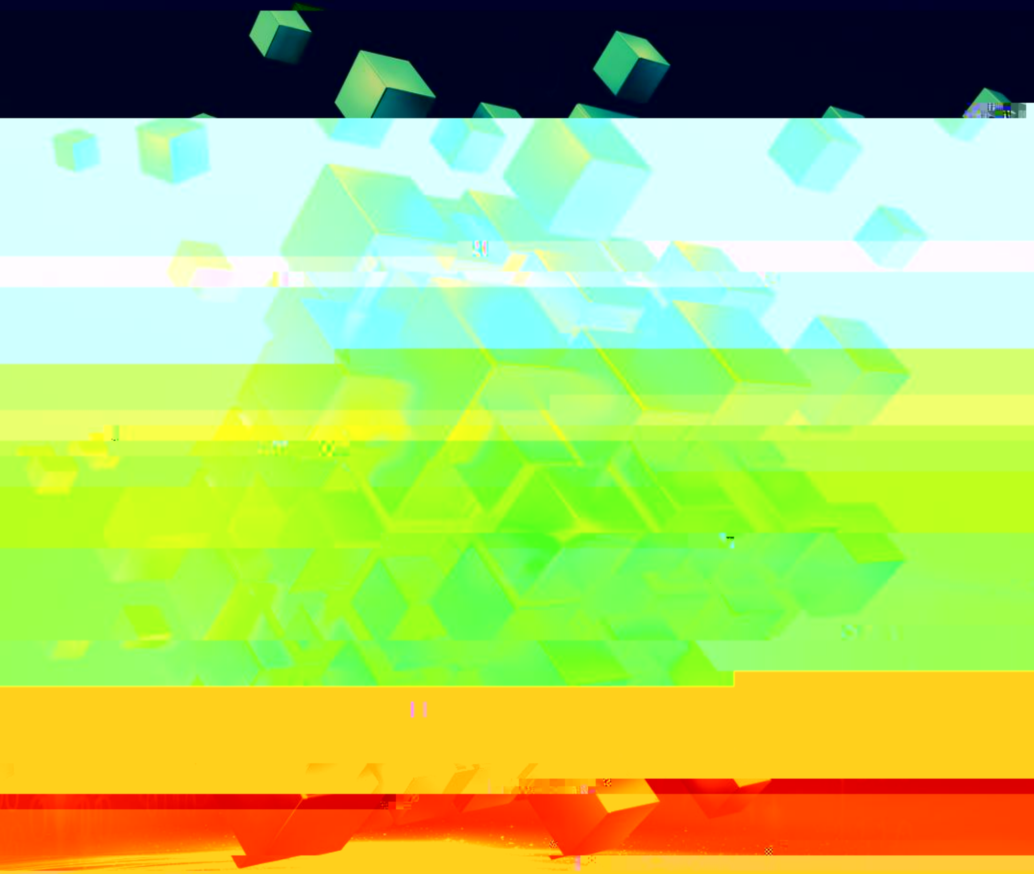
2021 WEST LAKE
CYBERSECURITY CONFERENCE
西湖论剑・网络安全大会



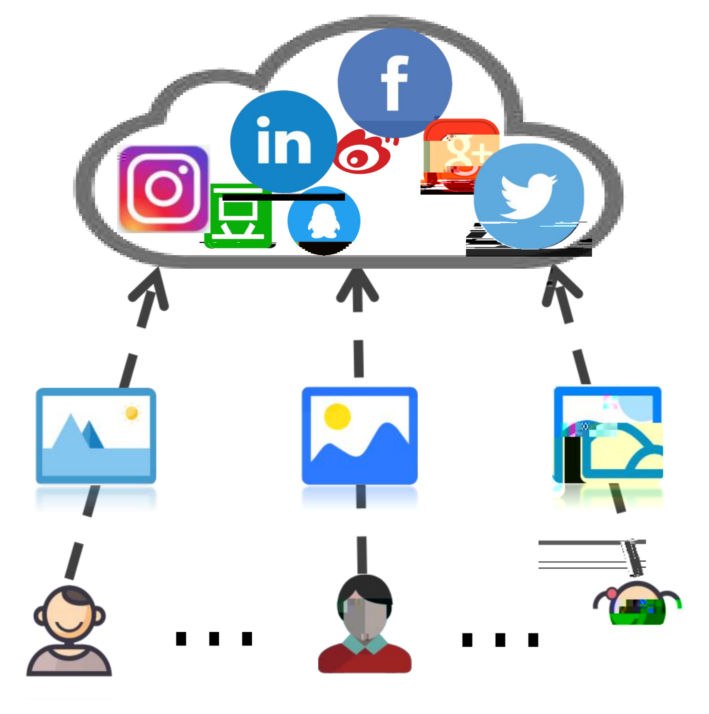
2021 CYBERSECURITY : THE FOUNDATION OF DIGITAL REFORM

“ ”

◗ փ ﬂ Ố ᒪ Ὼ ά

ᵶ ḙ ᒧ Ḡ ɰ ᐯ ḙ ᕠ

ģ ų˂ Ṯ ǎ ꝑ ɬ˜ ɺ Ѧ ╙ Φ ≠ و



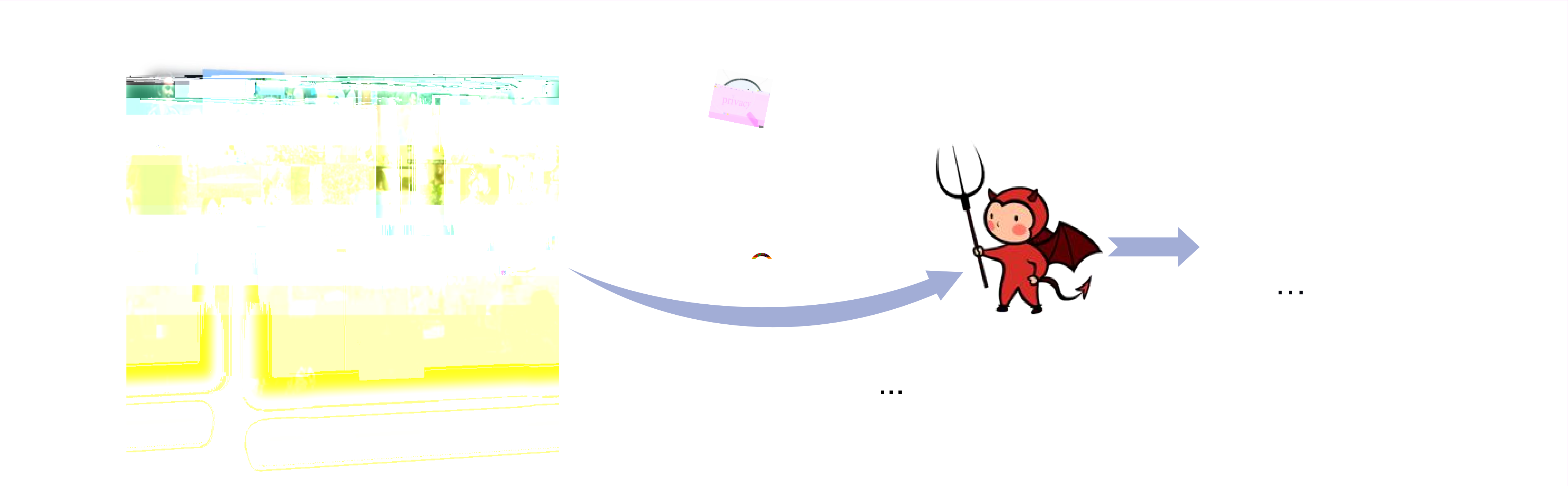
Facebook ⅛ ³ ẑ ɬ ῶ3 ắ Ł Ɑ [1]

Instagram ⅛ ³ ῶ ʌ ص9500 ắ Ł Ɑ ˙ ˊ

˙ ฿ Ṯ ɬ ῶ ʌ ص400 ắ Ł Ɑ q˂ [2]

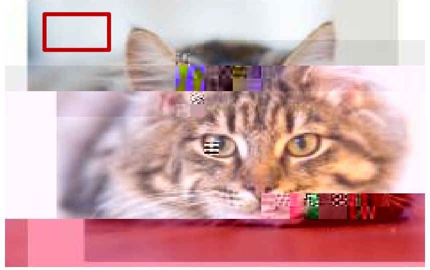
. ˠ Ĭ ˜ ⅛ ³ ῶ32 ắ ģ Ɑ q˂ [2]

[illegible]



Clearview AI [illegible] Facebook YouTube [illegible] Venmo [illegible] 30 [illegible] 600K [illegible]

[illegible]


[illegible]


chair
potted plant
orange
[illegible]


性别: 男
年龄: 57
表情: 喜上眉梢
魅力: 71
[illegible]


a red and white us parked in front of a building.
[illegible]

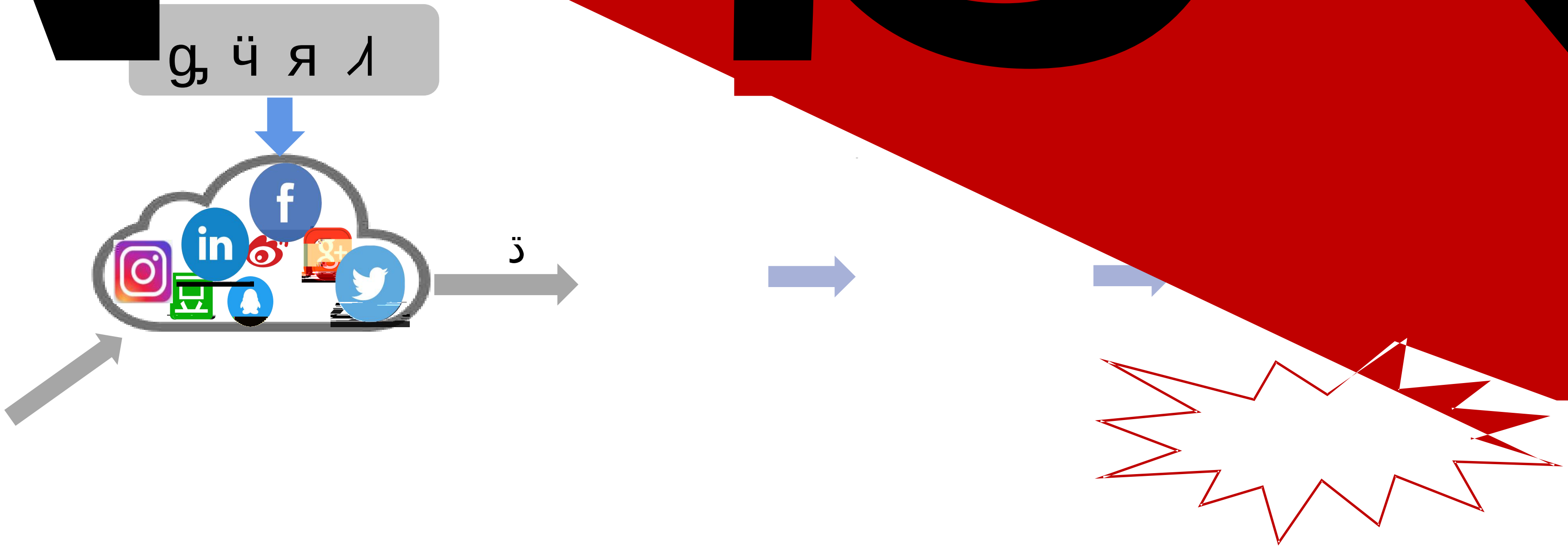
[illegible]

[illegible] DNNs [illegible]

Ḿ i ̉ i

ı я H ṛ ť

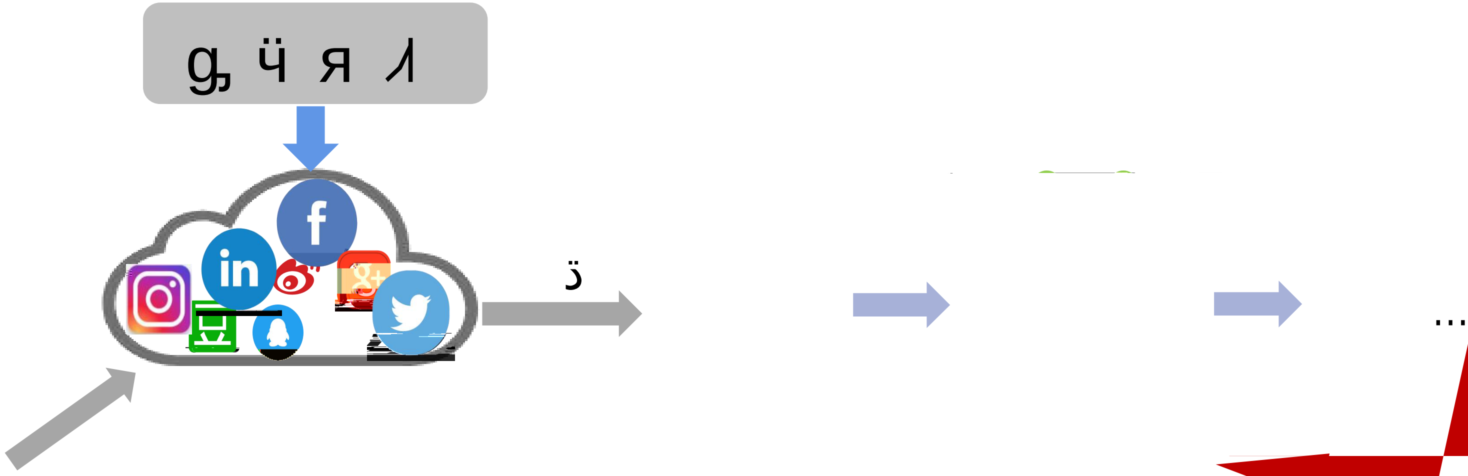
ʓ Ṁ ₇ Ḿ ı



Ḿ ỉ ớ ǥ ӵ ⅄ ص ῶ ̏Ω я ⅄ ª ̃ ⊐Ḿ ỉ ớ

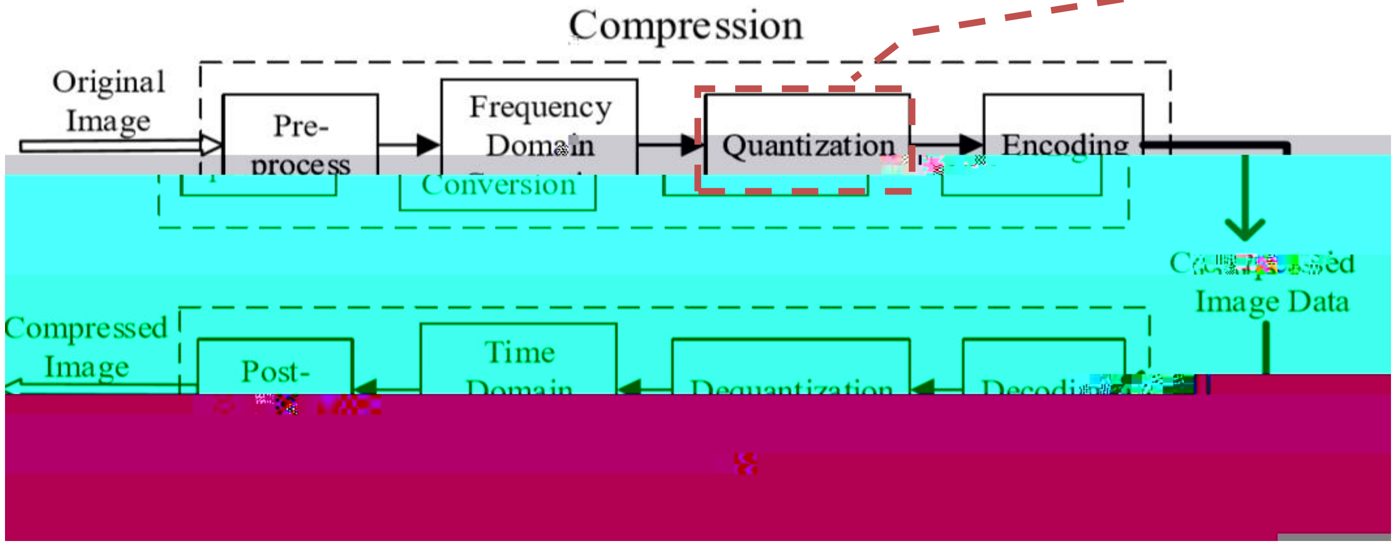
ǥ ӵ я ⅄ Ή ẍ ╒ Ẕ ὶ ˜ Ẉ ˩ ↑ ˋ ⅄ ڹ ˚ ◊ ⁼ ώ ܔ ц ڒ ῷ ' Ꞁ ḯ

‗ ڿ Ḿ ỉ ớ ῃ ʋ Ṁ₇ Ḿ ỉ ớ ǥ ӵ ῷ



[illegible]

[illegible]


Compression
Original Image
Pre-process
Frequency Domain Conversion
Quantization
Encoding
Compressed Image Data
Compressed Image
Post-
Time Domain
Dequantization
Decoding

[illegible]

[illegible]

[illegible]

ցӵ я ࢦ ⑊ | ￼ ˡ ỉ ἇ ˖ ˜ Ṁ₇ ǒ ˡ ἅ ỉ я ࢦ￼Ḿ ỉ ớ ցӵ

- ¡ Ḿ ցӵˋ ˡ ₩ ʒ [Seong et al. 2017]
- ¡ Ḿ´ ‰ ₅ ╜ ₩ ʒ [Liu et al. 2017]
- ¡ Ḿ ữ ∛ ̡ ₩ ʒ [Shawn et al. 2020]

JPEG [Richard et al. 2017]

پ ̈ ˡ ỉ ￼JPEG я ࢦ ⑊ | ₆ ˡ ỉ ẻ Ẫ

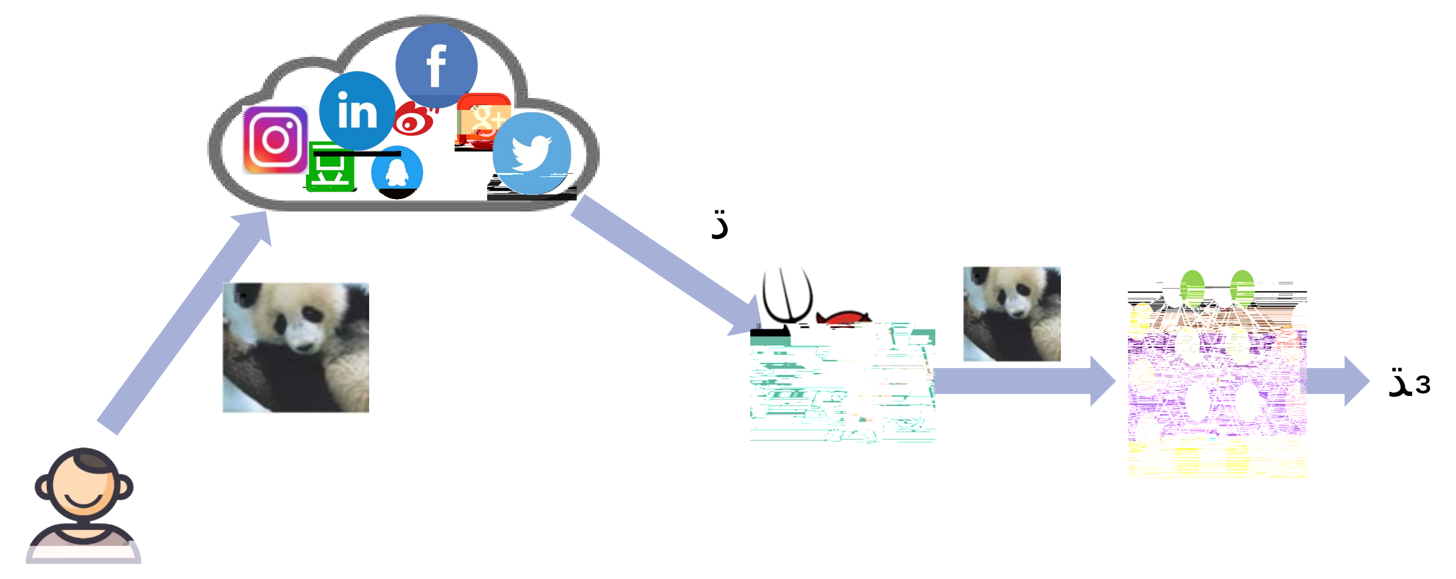
⌊ ∂ JPEG я ࢦ ⑊ | ̉ ҥ ѵ Ώ̦ ș

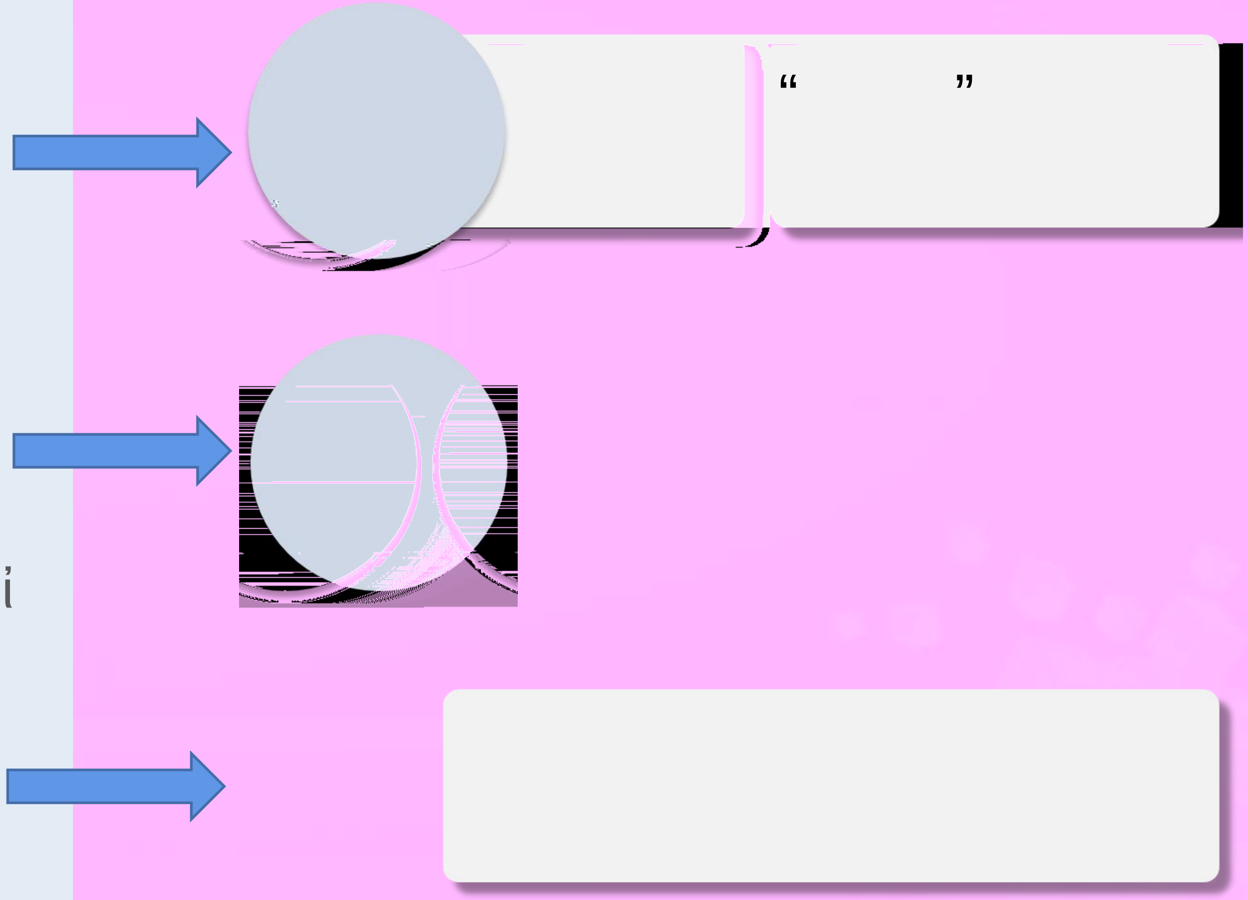
ώ ٦ ỉ я ⁄ Ḿ ỉ ớ ꞔ ч ı ᾰ Ά ḫ א ˜ ﻼ ᐱ ꞔ ч ڤ ٦ ĭ

ˋ Ḿ ỉ ớ ꞔ ч ئ Ṁ ῳ̈ ᾰ̈ n ệ ڃ ئ ڤ ٦ ụ

Ḿ ỉ ớ ꞔ ч ט ᶩ ỉ я ⁄ ớ ڗ ª ῆ Ὑ ט Ḿ ỉ ớ

ڲ ﺰ ª ˜ Ẉ ᒧ ט ῶ ỉ ʿ ˜ я ⁄ ʺ ڲ Ḿ ỉ ớ





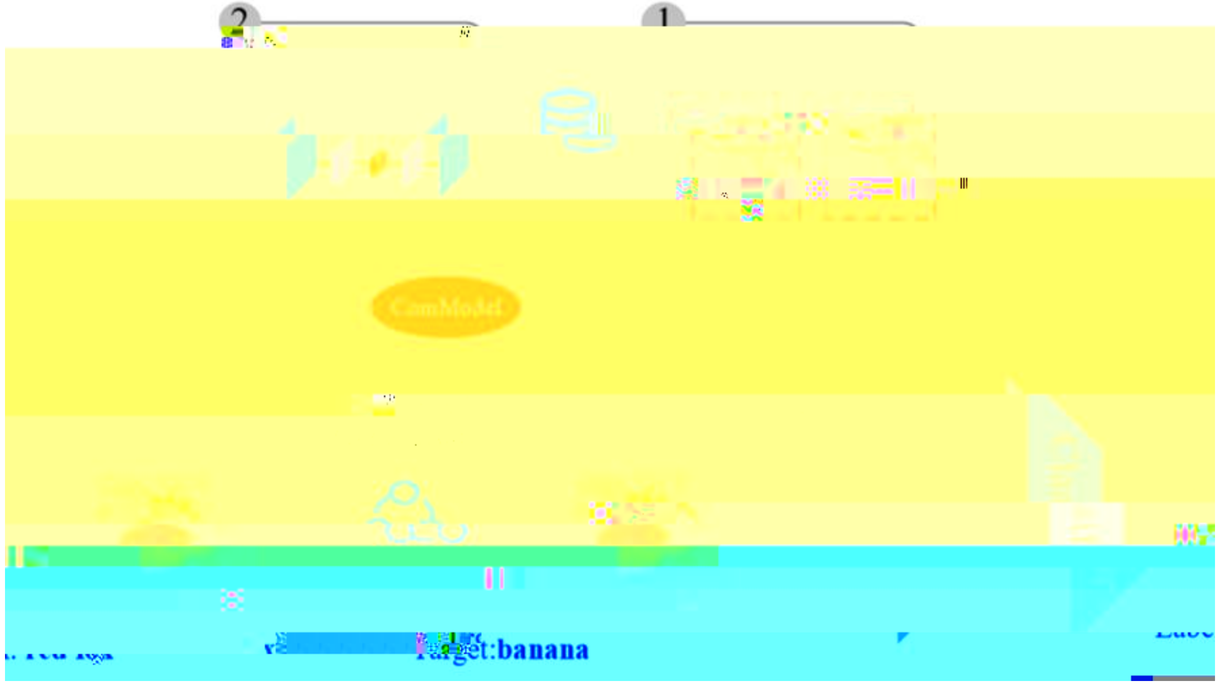
[illegible]

[illegible]

[illegible]

-ComReAdv

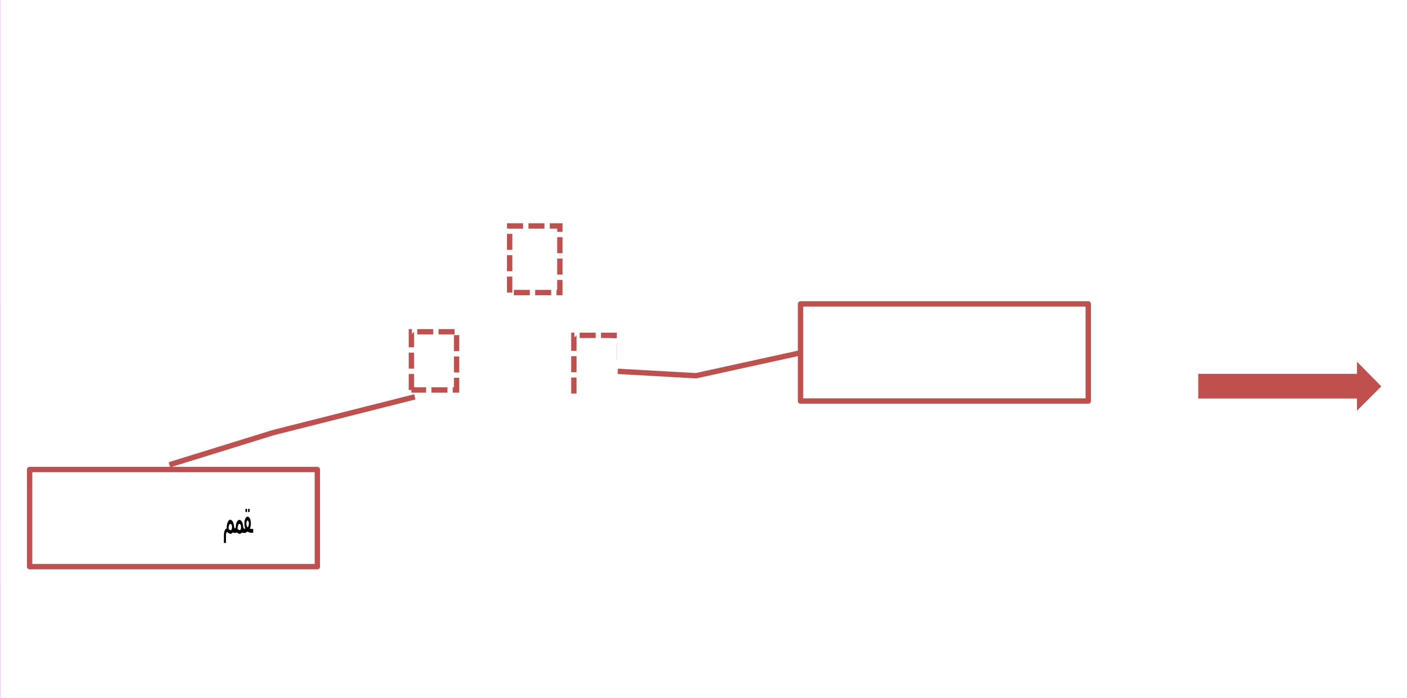
- [illegible]


2
1
CamModel
Target:banana

´ ‰ ɰ ẶḾ ỉ ¯ ￼ ỉ я ⅄ ớ

ֻ ḧ ᵇ Ḿ ỉ ¯ ئṀ₩ʒ ڙ˛ ڄئ￼˩ ʿ

ḧ ᵇ Ḿ ỉ ¯ ئṀ₩ʒ ڙ˛ ˮYḧ￼˩ ʿ



´ ‰ щ ĂḾ ỉ ¯ ỉ я ⅄ ớ

g FGSM[1], BIM[2], MIM[3] ∂ ȷ ộ ỳ ∂ ȷ ỉ я ⅄ Ḿ ỉ ¯ ק ´

‰

$$\arg\min_{r} ||r||_p$$

$$s.t.\ C(ComModel(x';\theta)) = t$$

$$x' = x + r \in [0,1]^n$$

→

$$r = sign\left(\nabla_x \mathcal{L}\left(C\left(ComModel(x;\theta)\right), t\right)\right),$$

$$x' = clip(x - \epsilon \cdot r)$$

$$r_{k+1} = sign\left(\nabla_x \mathcal{L}\left(C\left(ComModel(x_k;\theta)\right), t\right)\right),$$

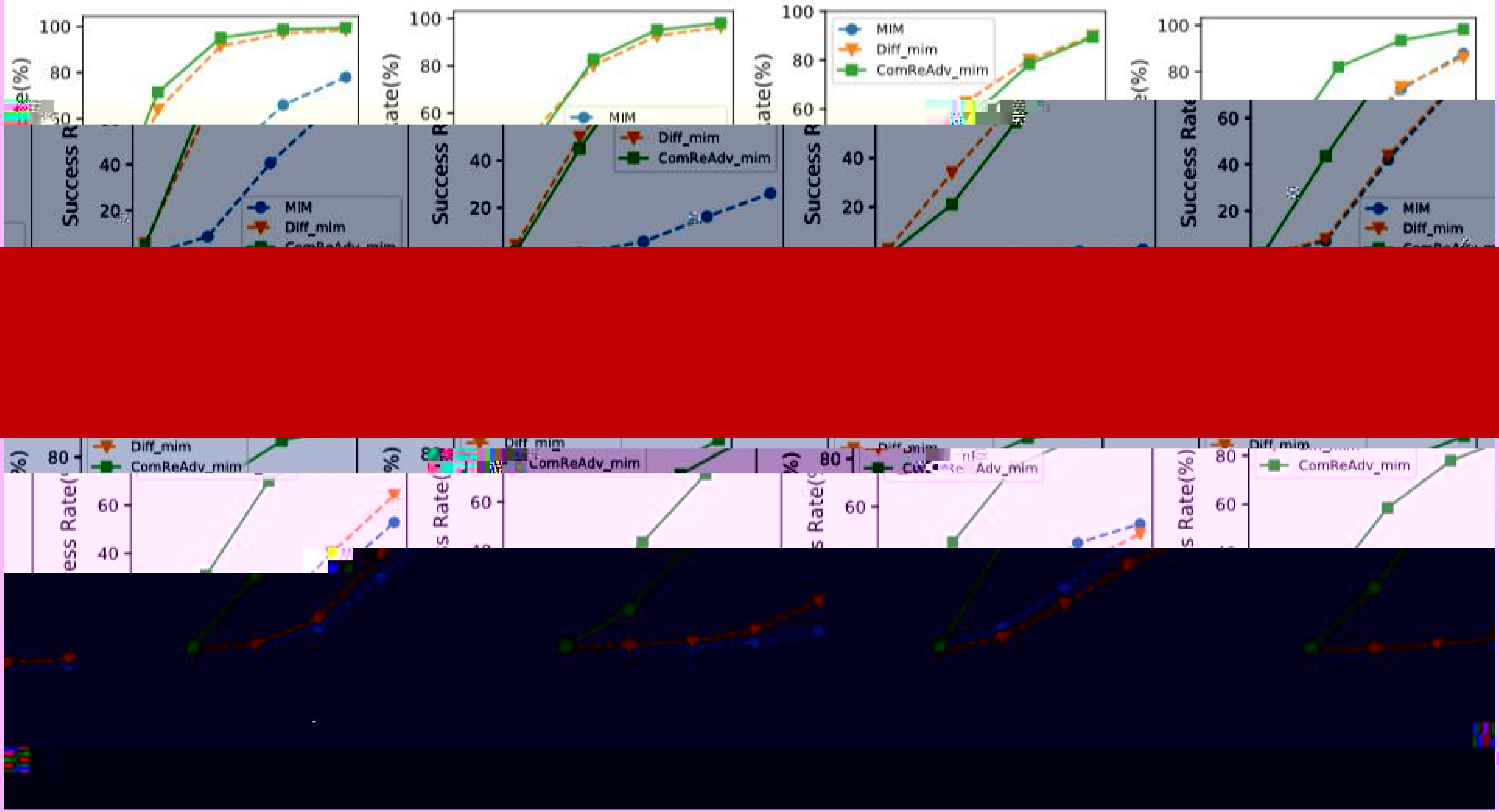
$$x_{k+1} = clip(x_k - \alpha \cdot r_{k+1}),\ x_0 = x$$

$$r_{k+1} = sign\left(\mu \cdot r_k + \nabla_x \mathcal{L}\left(C\left(ComModel(x_k;\theta)\right), t\right)\right),$$

$$x_{k+1} = clip(x_k - \alpha \cdot r_{k+1}),\ x_0 = x, r_0 = 0.$$

ComMode l d

（噪声幅度ϵ =5, 迭代次数10 ）

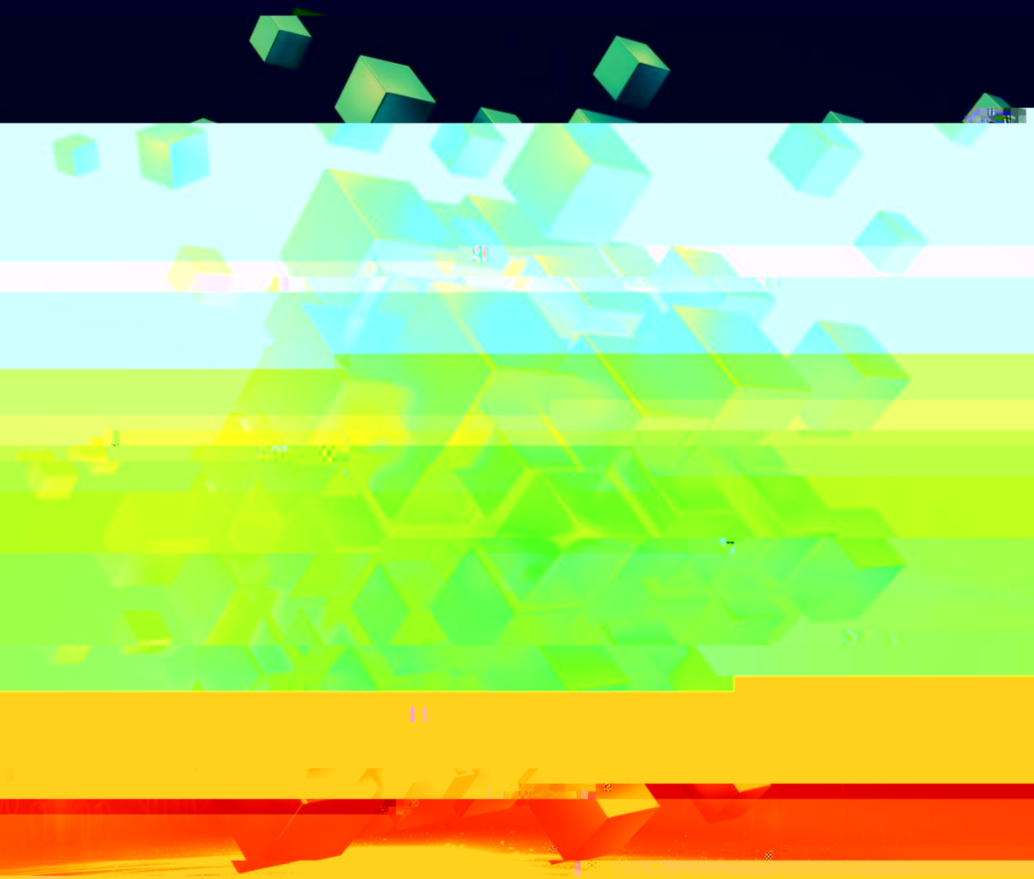

Success Rate(%)
100
80
60
40
20
MIM
Diff_mim
ComReAdv_mim

ỉ 3			
ظ א			

（噪声幅度 [illegible] 3，迭代次数10）

ỉ 3
ظ אִ

2021 WEST LAKE CYBERSECURITY CONFERENCE
西湖论剑·网络安全大会



2021 CYBERSECURITY：THE FOUNDATION OF DIGITAL REFORM