1 Robustness Certification for l_1 norm

Inspired by your insights, we have derived robustness guarantees for the l_1 norm utilizing the Laplacian smoothing distribution. According to our derivations, our method continues to address challenges such as paired input in visual GM and yields effective robustness certification results. However, as previously mentioned, such certification does not adequately preserve the inter-keypoint associations, which remains a challenge (C2 in the paper). For the pertinent proofs and quantified certification method, please refer to Sec. 1.1.

1.1 Proof for l_1 norm

In this section, we present the full proofs for the robustness guarantee for l_1 norm. The main tool for our proofs is the Neyman-Pearson lemma for two variables, which we establish in Lemma A.1 in the paper. Next, we prove Lemma 1.1, which is a special case of Lemma A.1 and states the Neyman-Pearson lemma for two Laplace noise variables. Based on this lemma, we obtain the certified result in Appendix 1.1.1.

Lemma 1.1 (Neyman-Pearson for Two Laplace Noise) *Let $X_1 \sim x_1 + \mathcal{L}(\lambda_1)$, $X_2 \sim x_2 + \mathcal{L}(\lambda_2)$ and $Y_1 \sim x_1 + \mathcal{L}(\lambda_1) + \delta_1$, $Y_2 \sim x_2 + \mathcal{L}(\lambda_2) + \delta_2$. Let $h : \mathbb{R}^d \times \mathbb{R}^d \to \{0, 1\}$ be any deterministic or random function. Then:*

1. *If $\mathcal{S}_1 \times \mathcal{S}_2 = \Big\{ z_1 \in \mathbb{R}^d, z_2 \in \mathbb{R}^d : \frac{1}{\lambda_1}(\|\boldsymbol{z_1} - \boldsymbol{\delta_1}\|_1 - \|\boldsymbol{z_1}\|_1) + \frac{1}{\lambda_2}(\|\boldsymbol{z_2} - \boldsymbol{\delta_2}\|_1 - \|\boldsymbol{z_2}\|_1)\Big) \geq \beta \}$ for some β and $P(h(X_1, X_2) = 1) \geq P((X_1, X_2) \in \mathcal{S}_1 \times \mathcal{S}_2)$, then $P(h(Y_1, Y_2) = 1) \geq P((Y_1, Y_2) \in \mathcal{S}_1 \times \mathcal{S}_2)$.*
2. *If $\mathcal{S}_1 \times \mathcal{S}_2 = \Big\{ z_1 \in \mathbb{R}^d, z_2 \in \mathbb{R}^d : \frac{1}{\lambda_1}(\|\boldsymbol{z_1} - \boldsymbol{\delta_1}\|_1 - \|\boldsymbol{z_1}\|_1) + \frac{1}{\lambda_2}(\|\boldsymbol{z_2} - \boldsymbol{\delta_2}\|_1 - \|\boldsymbol{z_2}\|_1)\Big) \leq \beta \}$ for some β and $P(h(X_1, X_2) = 1) \leq P((X_1, X_2) \in \mathcal{S}_1 \times \mathcal{S}_2)$, then $P(h(Y_1, Y_2) = 1) \leq P((Y_1, Y_2) \in \mathcal{S}_1 \times \mathcal{S}_2)$.*

This lemma is the special case of Neyman-Pearson for two variables when X_1, X_2, Y_1, and Y_2 are Laplace noises. It suffices to simply show that for any β, there is some $t > 0$ for which:

$$\left\{ z_1, z_2 : \frac{1}{\lambda_1}(\|\boldsymbol{z_1} - \boldsymbol{\delta_1}\|_1 - \|\boldsymbol{z_1}\|_1) + \frac{1}{\lambda_2}(\|\boldsymbol{z_2} - \boldsymbol{\delta_2}\|_1 - \|\boldsymbol{z_2}\|_1) \geq \beta \right\} = \left\{ z_1, z_2 : \frac{\mu_{Y_1}(z_1)\mu_{Y_2}(z_2)}{\mu_{X_1}(z_1)\mu_{X_2}(z_2)} \leq t \right\},$$
$$\left\{ z_1, z_2 : \frac{1}{\lambda_1}(\|\boldsymbol{z_1} - \boldsymbol{\delta_1}\|_1 - \|\boldsymbol{z_1}\|_1) + \frac{1}{\lambda_2}(\|\boldsymbol{z_2} - \boldsymbol{\delta_2}\|_1 - \|\boldsymbol{z_2}\|_1) \leq \beta \right\} = \left\{ z_1, z_2 : \frac{\mu_{Y_1}(z_1)\mu_{Y_2}(z_2)}{\mu_{X_1}(z_1)\mu_{X_2}(z_2)} \geq t \right\}. \tag{1}$$

$$\begin{aligned}
&\frac{\mu_{Y_1}(z_1)\mu_{Y_2}(z_2)}{\mu_{X_1}(z_1)\mu_{X_2}(z_2)} \\
&= \frac{\exp\left(-\frac{1}{\lambda_1}\|\boldsymbol{z_1} - \boldsymbol{\delta_1}\|_1\right)\exp\left(-\frac{1}{\lambda_2}\|\boldsymbol{z_2} - \boldsymbol{\delta_2}\|_1\right)}{\exp\left(-\frac{1}{\lambda_1}\|\boldsymbol{z_1}\|_1\right)\exp\left(-\frac{1}{\lambda_2}\|\boldsymbol{z_2}\|_1\right)} \\
&= \exp\left(-\frac{1}{\lambda_1}(\|\boldsymbol{z_1} - \boldsymbol{\delta_1}\|_1 - \|\boldsymbol{z_1}\|_1) - \frac{1}{\lambda_2}(\|\boldsymbol{z_2} - \boldsymbol{\delta_2}\|_1 - \|\boldsymbol{z_2}\|_1)\right)
\end{aligned}$$

By choosing $\beta = -\log(t)$, we can derive that

$$\frac{1}{\lambda_1}(\|\boldsymbol{z_1} - \boldsymbol{\delta_1}\|_1 - \|\boldsymbol{z_1}\|_1) + \frac{1}{\lambda_2}(\|\boldsymbol{z_2} - \boldsymbol{\delta_2}\|_1 - \|\boldsymbol{z_2}\|_1) \geq \beta \Longleftrightarrow \frac{\mu_{Y_1}(z_1)\mu_{Y_2}(z_2)}{\mu_{X_1}(z_1)\mu_{X_2}(z_2)} \leq t,$$
$$\frac{1}{\lambda_1}(\|\boldsymbol{z_1} - \boldsymbol{\delta_1}\|_1 - \|\boldsymbol{z_1}\|_1) + \frac{1}{\lambda_2}(\|\boldsymbol{z_2} - \boldsymbol{\delta_2}\|_1 - \|\boldsymbol{z_2}\|_1) \leq \beta \Longleftrightarrow \frac{\mu_{Y_1}(z_1)\mu_{Y_2}(z_2)}{\mu_{X_1}(z_1)\mu_{X_2}(z_2)} \geq t.$$

1.1.1 Proof of the Certified Robustness for l_1 norm

Theorem 1.2 (ℓ_1 norm certified space for visual GM) *Let f be a matching function, f_0 and g_0 be defined as in Eq.6 and Eq.7 in the paper, $\varepsilon_1 \sim \mathcal{L}(\lambda_1)$, $\varepsilon_2 \sim \mathcal{L}(\lambda_2)$. Suppose $\underline{p} \in (\frac{1}{2}, 1]$ satisfy:*

$$\begin{gathered}
P(f_0\left(\mathbf{c}^1, \mathbf{c}^2, \mathbf{z}^1 + \varepsilon_1, \mathbf{z}^2 + \varepsilon_2\right) = 1) = \\
P(f(\mathbf{c}^1, \mathbf{c}^2, \mathbf{z}^1 + \varepsilon_1, \mathbf{z}^2 + \varepsilon_2) \in \mathcal{X}') = p \geq \underline{p}.
\end{gathered} \tag{2}$$

Then we obtain the ℓ_1 *norm certified space for the perturbation pair* (δ_1, δ_2)*:*

$$\frac{\|\delta_1\|_1}{\lambda_1} + \frac{\|\delta_2\|_1}{\lambda_2} \leq -\log\left[2\left(1-\underline{p}\right)\right], \tag{3}$$

which guarantees $g_0\left(\mathbf{c}^1, \mathbf{c}^2, \mathbf{z}^1+\delta_1, \mathbf{z}^2+\delta_2\right) = 1$.

To show that $g_0\left(\mathbf{c}^1, \mathbf{c}^2, \mathbf{z}^1+\delta_1, \mathbf{z}^2+\delta_2\right) = 1$, it follows from the definition of g_0 that we need to show that:

$$P(f\left(\mathbf{c}^1, \mathbf{c}^2, \mathbf{z}^1+\varepsilon_1+\delta_1, \mathbf{z}^2+\varepsilon_2+\delta_2\right) \in \mathcal{X}') \geq P(f\left(\mathbf{c}^1, \mathbf{c}^2, \mathbf{z}^1+\varepsilon_1+\delta_1, \mathbf{z}^2+\varepsilon_2+\delta_2\right) \notin \mathcal{X}').$$

We define two random variables:

$$\begin{aligned} I &:= \left(\mathbf{c}^1, \mathbf{c}^2, \mathbf{z}^1+\varepsilon_1, \mathbf{z}^2+\varepsilon_2\right) \\ O &:= \left(\mathbf{c}^1, \mathbf{c}^2, \mathbf{z}^1+\varepsilon_1+\delta_1, \mathbf{z}^2+\varepsilon_2+\delta_2\right). \end{aligned}$$

We know that:

$$P(f(I) \in \mathcal{X}') \geq \underline{p}. \tag{4}$$

Our goal is to show that

$$P(f(O) \in \mathcal{X}') > P(f(O) \notin \mathcal{X}'). \tag{5}$$

Denote $T(\mathbf{z}^1, \mathbf{z}^2) = \frac{1}{\lambda_1}(\|\mathbf{z}^1 - \boldsymbol{\delta_1}\|_1 - \|\mathbf{z}^1\|_1) + \frac{1}{\lambda_2}(\|\mathbf{z}^2 - \boldsymbol{\delta_2}\|_1 - \|\mathbf{z}^2\|_1)$. Use Triangle Inequality we can derive a bound for $T(\mathbf{z}^1, \mathbf{z}^2)$:

$$-\frac{\|\delta_1\|_1}{\lambda_1} - \frac{\|\delta_2\|_1}{\lambda_2} \leq T(\mathbf{z}^1, \mathbf{z}^2) \leq \frac{\|\delta_1\|_1}{\lambda_1} + \frac{\|\delta_2\|_1}{\lambda_2}. \tag{6}$$

Pick β' such that there exists $B' \subseteq \{\boldsymbol{z_1}, \boldsymbol{z_2} : T(\boldsymbol{z_1}, \boldsymbol{z_2}) = \beta'\}$, and

$$P\left(I \in \{\boldsymbol{z_1}, \boldsymbol{z_2} : T(\boldsymbol{z_1}, \boldsymbol{z_2}) < \beta'\} \cup B'\right) = 1 - \underline{p} = P(f(I) \notin \mathcal{X}')). \tag{7}$$

Define

$$S := \{\boldsymbol{z_1}, \boldsymbol{z_2} : T(\boldsymbol{z_1}, \boldsymbol{z_2}) < \beta'\} \cup B', \tag{8}$$

so we also have $P(X \notin S) = p = P(f(I) \notin \mathcal{X}')$. Plug into Lemma 1.1, we can get

$$\begin{aligned} P(Y \notin S) &\leq P(f(O) \in \mathcal{X}'), \\ P(Y \in S) &\geq P(f(O) \notin \mathcal{X}'). \end{aligned} \tag{9}$$

Then we can obtain

$$\begin{aligned} \mathbb{P}(Y \in S) &= \int\int_S [2\lambda_1]^{-d}[2\lambda_2]^{-d} \exp\left(-\frac{\|\mathbf{z}^1 - \boldsymbol{\delta_1}\|_1}{\lambda_1}\right) \exp\left(-\frac{\|\mathbf{z}^2 - \boldsymbol{\delta_2}\|_1}{\lambda_2}\right) \mathrm{d}\mathbf{z}^1 \mathrm{d}\mathbf{z}^2 \\ &= \int\int_S [2\lambda_1]^{-d}[2\lambda_2]^{-d} \exp\left(-\frac{\|\mathbf{z}^1\|_1}{\lambda_1}\right)\left(-\frac{\|\mathbf{z}^2\|_1}{\lambda_2}\right) \exp\left(-T(\mathbf{z}^1, \mathbf{z}^2)\right) \mathrm{d}\mathbf{z}^1 \mathrm{d}\mathbf{z}^2 \\ &\leq \exp\left(\frac{\|\delta_1\|_1}{\lambda_1} + \frac{\|\delta_2\|_1}{\lambda_2}\right) \int\int_S [2\lambda_1]^{-d}[2\lambda_2]^{-d} \exp\left(-\frac{\|\mathbf{z}^1\|_1}{\lambda_1}\right)\left(-\frac{\|\mathbf{z}^2\|_1}{\lambda_2}\right) \mathrm{d}\mathbf{z}^1 \mathrm{d}\mathbf{z}^2 \\ &= \exp\left(\frac{\|\delta_1\|_1}{\lambda_1} + \frac{\|\delta_2\|_1}{\lambda_2}\right)(1-\underline{p}). \end{aligned} \tag{10}$$

Thus, if $\frac{\|\delta_1\|_1}{\lambda_1} + \frac{\|\delta_2\|_1}{\lambda_2} \leq -\log\left[2\left(1-\underline{p}\right)\right]$, it holds that

$$\begin{aligned} P(Y \in S) &\leq \exp\left(\frac{\|\delta_1\|_1}{\lambda_1} + \frac{\|\delta_2\|_1}{\lambda_2}\right)(1-\underline{p}) \\ &\exp\left(-\log\left[2\left(1-\underline{p}\right)\right]\right)(1-\underline{p}) \\ &= \frac{1}{2}. \end{aligned} \tag{11}$$

Table 1: ACR of RS-GM for NGMv2 on Pascal VOC under keypoint position perturbations. It shows the result for different λ_1 and λ_2, $s = 0.9$.

	$\lambda_1 = 0.5$,$\lambda_2 = 0.5$	$\lambda_1 = 0.5$,$\lambda_2 = 1$	$\lambda_1 = 1$,$\lambda_2 = 0.5$	$\lambda_1 = 1$,$\lambda_2 = 1$
ACR	9.342	17.708	18.033	34.571

1.2 Quantify Certification for l_1 norm

Moreover, by fixing one of δ_1 and δ_2 which is similar to in Sec.4.4, we simplify the joint space in Eq. 3 to a marginal space, which facilitates robustness evaluation. Specifically, we set one of δ_1 and δ_2 to be a zero matrix and derive a simple expression for Eq. 3. As an example, we consider the case of setting δ_2 to a zero matrix as follows:

$$\|\delta_1\|_1 \leq -\lambda_1 \log \left[2\left(1 - \underline{p}\right)\right]. \tag{12}$$

1.3 Experiment

We examine RS-GM on the Pascal VOC dataset for NGMv2 under keypoint position perturbations. We show the ACR for different distributions as Tab. 1, where λ_1 and λ_2 are the parameters for Laplace smoothing distributions. Tab. 1 demonstrates that our method is also capable of obtaining robustness certification for visual GM for l_1 norm. The parameters λ_1 and λ_2 are instrumental in balancing the robustness guarantee with the matching performance.

1.4 Reference in rebuttal

[1] Ren Q, Bao Q, Wang R, et al. Appearance and structure aware robust deep visual graph matching: Attack, defense and beyond[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 15263-15272.