Supplementary Material: Mixed-Bit Sampling Watermarking: Towards Unifying Stochastic Anti-Counterfeiting and Authentication in Copy Sensitive Graphical Code

Jiale Chen[1], Li Dong[1], Wei Wang[2,3], Rangding Wang[1], Weiwei Sun[4], Yushu Zhang[5], Jiantao Zhou[6]

[1]Department of Computer Science, Faculty of Electrical Engineering and Computer Science, Ningbo University, Ningbo, China
[2]Guangdong-Hong Kong-Macao Joint Laboratory for Emotion Intelligence and Pervasive Computing, Artificial Intelligence Research Institute, Shenzhen MSU-BIT University, Shenzhen, Guangdong, China
[3]School of Medical Technology, Beijing Institute of Technology, Beijing, China
[4]Alibaba Group, Zhejiang, China
[5]School of Computing and Artificial Intelligence, Jiangxi University of Finance and Economics, Nanchang, China
[6]State Key Laboratory of Internet of Things for Smart City, Department of Computer and Information Science, Faculty of Science and Technology, University of Macau, Macau, China
chenoly@foxmail.com, dongli@nbu.edu.cn, ehomewang@ieee.org, wangrangding@nbu.edu.cn, sunweiwei.sww@alibaba-inc.com, yushuboshi@163.com, jtzhou@umac.mo

I. Reliability and Efficiency of the MSW Framework

Reliability Evaluation: Recall that the texture patterns of 2LQR code are *deterministic*, which are all manually designed in a heuristic way. In contrast, the texture patterns generated by the proposed MSW framework are inherently *stochastic*. Thus, the reliability of the MSW framework need to be validated. We evaluated the reliability of MSW-D CDP and MSW-P QR code using the following three metrics.

Reliability metric for white pixel ratio hyper-parameter α: We propose a metric that assesses the deviation in the white pixel ratio between the generated texture patterns and the pre-specified hyper-parameter α for both MSW-D CDP and MSW-P QR code, which can be expressed as,

$$\bar{\alpha} = \left| \frac{\sum_{\mathbf{x}} \mathbf{P}^g(\mathbf{x})}{N^2} - \alpha \right|, \tag{1}$$

where $\mathbf{P}^g$ represents the texture pattern generated by the proposed MSW framework, and α is the user-specified white pixel ratio. **Reliability metric for embedding strength Hyper-parameter δ:** We propose a metric to evaluate the deviation in embedding strength for MSW-D CDP between the generated texture pattern and the user provided hyper-parameter δ, which is defined as

$$\bar{\delta} = \left| \phi(\mathbf{P}^g, u, v) - \delta \right|, \tag{2}$$

where $\phi(\cdot)$ is the DCT coefficient difference.

Reliability metric for Pearson hyper-parameter γ: This metric measures the deviation in Pearson similarity between the generated texture pattern and the user-specified given hyper-parameter γ, which can be expressed as

$$\bar{\gamma} = \frac{1}{q} \sum_{m=1}^{q} \sum_{n=m+1}^{q} \left| \text{corr}(\mathbf{P}_i^m, \mathbf{P}_i^n) - \gamma \right|, \tag{3}$$

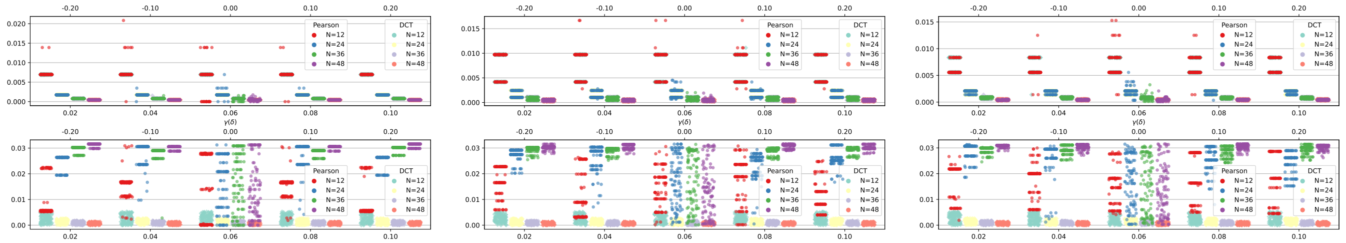
where $\texttt{corr}(\cdot)$ is the Pearson coefficient function and $\mathbf{P}_i^m, \mathbf{P}_i^n \in \mathcal{P}_i$.

We evaluated the $\bar{\alpha}, \bar{\delta}$, and $\bar{\gamma}$ for the proposed MSW-D CDP and MSW-P QR code on a dataset. The hyper-parameter combination of this dataset that similar to **Dataset #3** and **Dataset #4** and has 100 texture patterns.

Fig. 1 illustrates the metric distribution across various hyper-parameter combinations. The results demonstrate that for hyper-parameter α, both MSW-D CDP and MSW-P QR code exhibit a gradually decreasing error as N increases. The majority of $\bar{\alpha}$ values are smaller than 0.01, and the metric distributions for both schemes appear to be quite similar. This verified that the proposed MSW framework could provide a precise and accurate control over the white pixel ratio. Moreover, the $\bar{\delta}$ values are shown at the bottom of Fig. 1. For MSW-P QR code, the results show that, regardless of the hyper-parameter combination, the values of $\bar{\gamma}$ are consistently close to 0. Although the $\bar{\delta}$ for MSW-D CDP exceeds the γ for MSW-P QR code, for all hyper-parameter combinations, the maximum value of $\bar{\delta}$ still attains a small number, *i.e.*, 0.032.

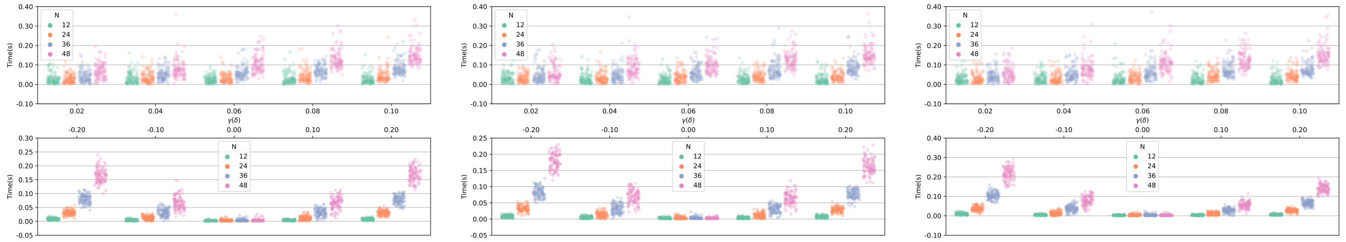
Overall, the experiments demonstrate that the proposed MSW framework performs well in terms of reliability, showing a highly accurate control for the hyper-parameters α, δ and γ. This lays a solid foundation for a practical usage of the proposed MSW framework.

Computational Cost: The time complexity of the proposed method is evaluated under the following setting: Intel Core i5-10500 CPU, Python 3.7, NumPy 1.21.6, PyTorch 1.13.1. Note that the complexity is also affected by several hyper-parameters, *i.e.,* the texture pattern size N, embedding strength γ and the white pixels ratio α. For each hyper-parameter combination, we generate digital texture patterns for 100 times, and the distribution of the generation time cost is shown in Fig. 2, The top and the bottom rows are for MSW-D CDP and MSW-P



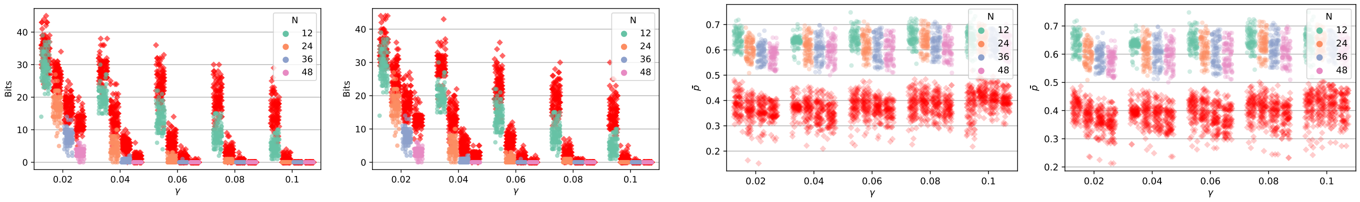
(a) $\alpha = 0.5$ (b) $\alpha = 0.6$ (c) $\alpha = 0.7$

Fig. 1. Reliability metrics distributions for different hyper-parameter combinations evaluated using the MSW framework. The top sub-figure and the bottom sub-figure are shown for $\bar{\alpha}$ and $\bar{\delta}$, $\bar{\gamma}$ respectively.



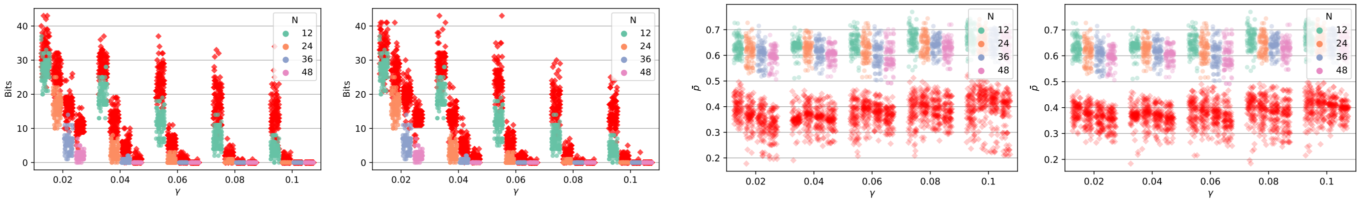
(a) $\alpha = 0.5$ (b) $\alpha = 0.6$ (c) $\alpha = 0.7$

Fig. 2. Time complexity analysis of the MSW framework for various hyper-parameter combinations. The top sub-figure displays the generation times for MSW-D CDP, while the bottom sub-figure shows results for MSW-P QR code.



(a) NEB (**BinAttack**) (b) NEB (**NetAttack**) (c) $\bar{p}$ (**BinAttack**) (d) $\bar{p}$ (**NetAttack**)

Fig. 3. Visualization of NEB distributions and their linear separability under different attacks with $\alpha = 0.6$ for MSW-D CDP. (a) and (b) show the NEB distributions under **BinAttack** and **NetAttack** attacks, respectively. (c) and (d) illustrate the linear separability of $\bar{p}$ values under the same attacks.



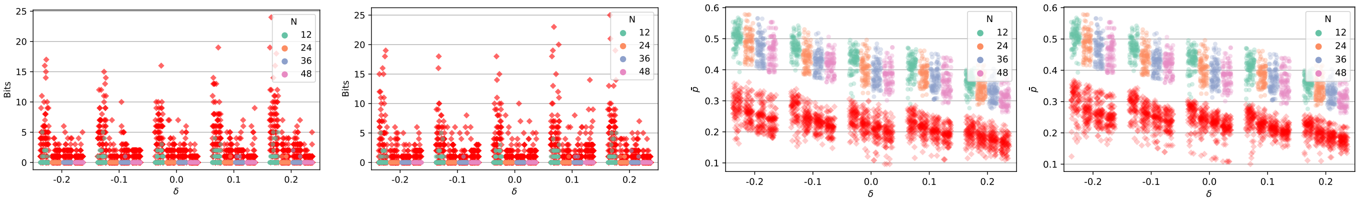
(a) NEB (**BinAttack**) (b) NEB (**NetAttack**) (c) $\bar{p}$ (**BinAttack**) (d) $\bar{p}$ (**NetAttack**)

Fig. 4. Visualization of NEB distributions and their linear separability under different attacks with $\alpha = 0.7$ for MSW-D CDP. (a) and (b) show the NEB distributions under **BinAttack** and **NetAttack** attacks, respectively. (c) and (d) illustrate the linear separability of $\bar{p}$ values under the same attacks.

QR code, respectively. One can see that the cost times mainly effected by the hyper-parameter N. For both MSW-D CDP and MSW-P QR code, the time cost required to generate texture patterns is generally less than $0.25s$. Furthermore, based on the recommended hyper-parameters obtained in the Section V-C, *i.e.*, $N = 48$ and $\gamma = 0.02$, the average generation time for MSW-D CDP is significantly reduced to $0.056s$, which could meets practical usage in the real-world scenario.

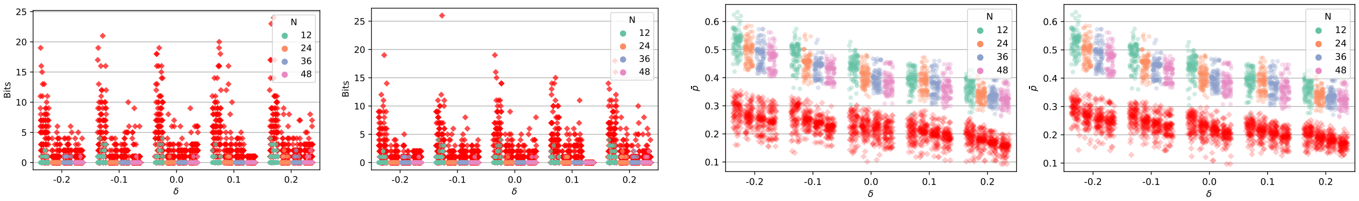
II. More results for Hyper-parameter Selection

In the Section of hyper-parameter selection, we only give the experimental results about $\alpha = 0.5$. In order to find the change of different authentication scores for different α.



(a) NEB (**BinAttack**) (b) NEB (**NetAttack**) (c) $\bar{p}$ (**BinAttack**) (d) $\bar{p}$ (**NetAttack**)

Fig. 5. Visualization of NEB distributions and their linear separability under different attacks with $\alpha = 0.6$ for MSW-P QR code. (a) and (b) show the NEB distributions for **BinAttack** and **NetAttack** attacks, respectively. (c) and (d) illustrate the linear separability of $\bar{p}$ values for the respective attacks.



(a) NEB (**BinAttack**) (b) NEB (**NetAttack**) (c) $\bar{p}$ (**BinAttack**) (d) $\bar{p}$ (**NetAttack**)

Fig. 6. Visualization of NEB distributions and their linear separability under different attacks with $\alpha = 0.7$ for MSW-P QR code. (a) and (b) show the NEB distributions for **BinAttack** and **NetAttack** attacks, respectively. (c) and (d) illustrate the linear separability of $\bar{p}$ values for the respective attacks.