Watermarking One for All: A Robust Watermarking Scheme Against Partial Image Theft

Supplementary Material

1. Overview

Due to the 8-page submission limit for CVPR, we are unable to present all the content in the main paper. Therefore, we provided the sub-significant content in the supplementary materials. The supplementary material is arranged as follows. In Section 2, we will present more intuitive results for visual performance. In Section 3, we are going to present more experimental results about robustness against partial image theft. In Section 4, we will try to analysis the newly presented results.

2. Visual Performance (Supplement)

We have present some watermarked images embedded by different methods in Fig.5. Here, we will present more results to better demonstrate the good visual performance achieved by our scheme, as shown in Fig.8.

3. Robustness against Partial Image Theft (Supplement)

In this section, we present the results of four more experiments. Firstly, we compare the robustness performance under different common distortions in digital channel. The results are illustrated in Table 7. As shown, since our work focuses on dealing with partial image theft, the distortion layer does not include many attacks in the digital channel, so the performance is slightly inferior to other solutions, yet the overall performance is acceptable.

Table 7. Bit accuracy rate(BAR,%) under different common distortions in digital channel

Methods	Clean	JPEG(QF)		Gaussian(σ)		Blur(kernel)		Resizing(%)	
		95	85	0.01	0.05	3×3	5×5	50	200
HiDDeN	90.51	80.73	73.59	90.52	90.52	86.08	81.47	81.62	90.51
DWSF	99.99	99.98	99.59	99.99	99.99	99.99	99.99	99.99	99.99
MBRS	100	100	99.99	100	100	100	100	100	100
PIMoG	99.92	99.01	93.50	99.93	99.94	99.88	99.67	99.92	99.94
StegaStamp	98.93	98.56	97.35	98.93	98.93	98.91	98.83	98.85	98.93
WOFA	98.39	91.87	87.23	95.89	95.89	96.82	90.69	82.21	95.89

As a supplement for Table 4 and Table 5, we adopt more detailed experimental settings and conduct experiments accordingly. In Table 8, we test several methods across 15 experimental combinations, using 3 levels of translation ratio and 5 levels of partial masking ratio. In Table 9, we test these methods across 15 experimental combinations, using 3 levels of rotation angles and 5 levels of partial masking ratio. In Table 10, we test these methods across 15 experimental combinations, using 3 levels of scaling ratio and 5 levels of partial masking ratio. As illustrated in all three tables, our scheme achieves superior performance across all settings, thus showing its reliability on tackling the challenge of partial image theft.

4. Analysis (Supplement)

In this section, we will try to analyze the experimental results and further explore the problem of partial image theft.

4.1. Why MBRS shows good performance?

As shown in Table 4 and Table 8 achieve good performance especially when only partial masking is performed. We believe that this is caused by the unique diffusion block of MBRS [13]. MBRS diffuses the watermark message to the entire image, therefore gains the ability to combat partial masking. This process can also be found in Fig.5, where the residuals of MBRS are evenly distributed throughout the image. Although this operation may affect the visual effect to some extent, it does compensate in terms of robustness.

4.2. Why MuST fall short?

The newly proposed method MuST [23] does not performed well in our experiments. This does not mean that MuST's ability is poor, but it just does not fit well in our experimental scenarios. The reason is that MuST embed watermarks into the protected object, while partial masking is a random process in our definition. Therefore, the partial masking process often excludes the area containing the watermark, so the extraction performance is affected. We set it up this way because we believe that the protector cannot predict in advance how the attacker will steal the image. Or in other words, we consider the worst case.

4.3. Why StegaStamp perform better against rotation and scaling?

As shown in Table 9 and Table 10, StegaStamp [21] performs quite well against rotation and scaling under high partial masking ratio. We believe that StegaStamp's use of perspective transforms in its distortion layer contributes to this effect. To combat perspective distortion in image capture, StegaStamp applies a perspective transformation attack, which may include rotation and scaling. As a result, it performs better when the partial masking ratio is high. However, at lower masking ratios, content loss becomes more significant, leading to performance degradation.

Figure 8. Visualization of watermarked images embedded by different methods. Our WOFA achieves satisfying visual performance overall.

Table 8. Bit accuracy rate(BAR,%) under different Translation-Partial masking pairs in Partial Image Theft.

Methods	Clean	Translation 10% + Partial Masking(%)					Translation 25% + Partial Masking(%)					Translation 50% + Partial Masking(%)				
		(0, 20]	(20, 40]	(40, 60]	(60, 80]	(80, 100)	(0, 20]	(20, 40]	(40, 60]	(60, 80]	(80, 100)	(0, 20]	(20, 40]	(40, 60]	(60, 80]	(80, 100)
DWSF	99.99	49.93	50.08	51.58	57.41	65.08	49.93	49.81	49.92	49.69	49.62	50.08	49.96	49.96	49.92	49.99
MBRS	100	52.78	57.45	60.58	62.07	63.55	56.63	60.82	61.37	63.13	63.81	51.08	53.06	53.33	53.02	53.31
PIMoG	99.92	52.07	57.69	61.77	65.05	67.61	48.90	46.43	45.50	44.62	43.77	50.35	50.95	51.17	51.75	51.42
StegaStamp	98.93	52.01	55.85	59.25	62.06	64.41	49.86	49.38	48.93	48.79	48.38	49.83	49.57	49.82	49.40	49.50
MuST	99.59	50.03	50.06	49.66	50.55	50.24	49.98	50.17	49.79	49.78	49.74	50.12	49.86	50.12	50.22	49.90
WOFA	98.39	**86.14**	**97.91**	**98.68**	**98.41**	**98.39**	**87.56**	**98.33**	**98.82**	**98.61**	**98.43**	**77.63**	**96.10**	**98.06**	**98.25**	**98.62**

Table 9. Bit accuracy rate(BAR,%) under different Rotation-Partial masking pairs in Partial Image Theft.

Methods	Clean	Rotation 15° + Partial Masking(%)					Rotation 30° + Partial Masking(%)					Rotation 45° + Partial Masking(%)				
		(0, 20]	(20, 40]	(40, 60]	(60, 80]	(80, 100)	(0, 20]	(20, 40]	(40, 60]	(60, 80]	(80, 100)	(0, 20]	(20, 40]	(40, 60]	(60, 80]	(80, 100)
DWSF	99.99	49.89	49.77	50.19	51.24	52.75	50.00	49.92	49.98	49.53	49.83	49.95	49.94	50.07	49.80	49.77
MBRS	100	50.04	50.11	50.68	50.81	50.17	49.94	50.36	50.45	50.46	50.30	49.74	49.53	49.24	49.13	49.00
PIMoG	99.92	50.03	49.62	48.76	49.16	49.24	50.29	50.04	49.96	49.95	50.58	49.89	50.05	50.23	50.27	50.32
StegaStamp	98.93	52.35	58.54	61.82	63.11	62.99	50.35	51.26	51.71	51.15	51.13	50.05	50.10	50.07	49.86	50.10
MuST	99.59	50.18	50.33	49.91	49.82	50.44	49.91	50.01	49.66	50.02	50.11	50.02	50.25	50.05	49.70	49.98
WOFA	98.39	**87.08**	**99.45**	**99.63**	**99.49**	**99.06**	**85.24**	**98.98**	**99.28**	**99.11**	**98.75**	**79.35**	**96.30**	**96.95**	**96.46**	**95.89**

Table 10. Bit accuracy rate(BAR,%) under different Scaling-Partial masking pairs in Partial Image Theft.

Methods	Clean	Scaling ±10% + Partial Masking(%)					Scaling ±20% + Partial Masking(%)					Scaling ±25% + Partial Masking(%)				
		(0, 20]	(20, 40]	(40, 60]	(60, 80]	(80, 100)	(0, 20]	(20, 40]	(40, 60]	(60, 80]	(80, 100)	(0, 20]	(20, 40]	(40, 60]	(60, 80]	(80, 100)
DWSF	99.99	49.85	50.35	52.24	57.57	65.33	49.88	50.06	51.24	54.31	58.74	49.89	50.18	51.19	53.44	57.14
MBRS	100	50.15	52.02	51.59	49.30	48.05	50.00	50.27	50.27	49.64	49.80	50.00	50.08	50.06	49.84	50.07
PIMoG	99.92	53.90	64.46	70.62	74.09	75.07	50.17	51.34	50.93	50.11	48.72	50.12	50.25	49.43	49.24	48.38
StegaStamp	98.93	56.25	72.35	82.54	89.09	93.27	53.58	63.62	68.96	72.03	73.49	52.67	60.10	63.90	65.69	65.95
MuST	99.59	49.89	49.99	50.21	50.04	50.19	50.01	49.90	50.15	49.85	50.16	50.02	49.95	50.01	49.97	49.97
WOFA	98.39	**88.77**	**99.76**	**99.84**	**99.81**	**99.73**	**87.35**	**99.69**	**99.81**	**99.74**	**99.75**	**86.40**	**99.53**	**99.74**	**99.79**	**99.69**