

NISTIR XXXX Draft

Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification

Patrick Grother
Mei Ngan
Kayee Hanaoka
*Information Access Division
Information Technology Laboratory*

This publication is available free of charge from:
<https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing>

2018/01/25

DISCLAIMER

Specific hardware and software products identified in this report were used in order to perform the evaluations described in this document. In no case does identification of any commercial product, trade name, or vendor, imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products and equipment identified are necessarily the best available for the purpose.

ABOUT THIS REPORT

This report is a draft NIST Interagency Report, and is open for comment. It documents the verification-track of the ongoing Face Recognition Vendor Test. The report will be updated continuously as new algorithms are evaluated, as new datasets are added, and as new analyses are included. Comments and suggestions should be directed to frvt@nist.gov.

Contents

DISCLAIMER	1
1 NEWS	6
2 CHANGELOG	6
3 METRICS	12
3.1 CORE ACCURACY	12
4 DATASETS	13
4.1 CHILD EXPLOITATION IMAGES	13
4.2 VISA IMAGES	13
4.3 MUGSHOT IMAGES	13
4.4 SELFIE IMAGES	14
4.5 WEBCAM IMAGES	14
4.6 WILD IMAGES	15
5 RESULTS	15
5.1 TEST GOALS	15
5.2 TEST DESIGN	15
5.3 FAILURE TO ENROL	18
5.4 RECOGNITION ACCURACY	19
5.5 GENUINE DISTRIBUTION STABILITY	37
5.5.1 EFFECT OF BIRTH PLACE ON THE GENUINE DISTRIBUTION	37
5.5.2 EFFECT OF AGE ON GENUINE SUBJECTS	39
5.6 IMPOSTOR DISTRIBUTION STABILITY	41
5.6.1 EFFECT OF BIRTH PLACE ON THE IMPOSTOR DISTRIBUTION	41
5.6.2 EFFECT OF AGE ON IMPOSTORS	144

List of Tables

1 ALGORITHM SUMMARY	8
2 FALSE NON-MATCH RATE	9
3 FAILURE TO ENROL RATES	18

List of Figures

1 PERFORMANCE SUMMARY: FNMR VS. TEMPLATE SIZE TRADEOFF	10
2 PERFORMANCE SUMMARY: FNMR VS. TEMPLATE TIME TRADEOFF	11
3 EXAMPLE IMAGES	15
(A) VISA	15
(B) MUGSHOT	15
(C) WEBCAM	15
(D) SELFIE	15
(E) WILD	15
4 ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES	20
5 ERROR TRADEOFF CHARACTERISTIC: VISA IMAGES	21
6 ERROR TRADEOFF CHARACTERISTIC: MUGSHOT IMAGES	22
7 ERROR TRADEOFF CHARACTERISTIC: SELFIE IMAGES	23
8 ERROR TRADEOFF CHARACTERISTIC: SELFIE IMAGES	24

9	ERROR TRADEOFF CHARACTERISTIC: WILD IMAGES	25
10	PERFORMANCE SUMMARY: FNMR VS. YAW ANGLE	26
11	PERFORMANCE SUMMARY: FMR VS. YAW ANGLE	27
12	ERROR TRADEOFF CHARACTERISTICS: CHILD EXPLOITATION IMAGES	28
13	CMC CHARACTERISTICS: CHILD EXPLOITATION IMAGES	29
14	CMC CHARACTERISTICS: CHILD EXPLOITATION IMAGES	30
15	SEX AND RACE EFFECTS: MUGSHOT IMAGES	31
16	SEX EFFECTS: VISA IMAGES	32
17	ERROR TRADEOFF CHARACTERISTIC: WILD IMAGES	33
18	FALSE MATCH RATE CALIBRATION: VISA IMAGES	34
19	FALSE MATCH RATE CONCENTRATION: VISA IMAGES	35
20	FALSE MATCH RATE CALIBRATION: MUGSHOT IMAGES	36
21	EFFECT OF COUNTRY OF BIRTH ON FNMR	38
22	EFFECT OF SUBJECT AGE ON FNMR	40
23	WORST CASE REGIONAL EFFECT FNMR	42
24	IMPOSTOR DISTRIBUTION SHIFTS FOR SELECT COUNTRY PAIRS	44
25	ALGORITHM 3DIVI-001 CROSS REGION FMR	45
26	ALGORITHM 3DIVI-002 CROSS REGION FMR	46
27	ALGORITHM AWARE-000 CROSS REGION FMR	47
28	ALGORITHM AWARE-001 CROSS REGION FMR	48
29	ALGORITHM AYONIX-000 CROSS REGION FMR	49
30	ALGORITHM CAMVI-001 CROSS REGION FMR	50
31	ALGORITHM COGENT-000 CROSS REGION FMR	51
32	ALGORITHM CYBEREXTRUDER-001 CROSS REGION FMR	52
33	ALGORITHM DERMALOG-003 CROSS REGION FMR	53
34	ALGORITHM DERMALOG-004 CROSS REGION FMR	54
35	ALGORITHM DIGITALBARRIERS-000 CROSS REGION FMR	55
36	ALGORITHM DIGITALBARRIERS-001 CROSS REGION FMR	56
37	ALGORITHM FDU-000 CROSS REGION FMR	57
38	ALGORITHM FDU-001 CROSS REGION FMR	58
39	ALGORITHM ID3-001 CROSS REGION FMR	59
40	ALGORITHM ID3-002 CROSS REGION FMR	60
41	ALGORITHM INNOVATRICES-000 CROSS REGION FMR	61
42	ALGORITHM INNOVATRICES-001 CROSS REGION FMR	62
43	ALGORITHM INTELLIVISION-001 CROSS REGION FMR	63
44	ALGORITHM ISITYOU-000 CROSS REGION FMR	64
45	ALGORITHM ISYSTEMS-000 CROSS REGION FMR	65
46	ALGORITHM ITMO-002 CROSS REGION FMR	66
47	ALGORITHM MORPHO-000 CROSS REGION FMR	67
48	ALGORITHM MORPHO-002 CROSS REGION FMR	68
49	ALGORITHM NEUROTECHNOLOGY-001 CROSS REGION FMR	69
50	ALGORITHM NEUROTECHNOLOGY-002 CROSS REGION FMR	70
51	ALGORITHM NOBLIS-000 CROSS REGION FMR	71
52	ALGORITHM NTECHLAB-002 CROSS REGION FMR	72
53	ALGORITHM NTECHLAB-003 CROSS REGION FMR	73
54	ALGORITHM PA-002 CROSS REGION FMR	74
55	ALGORITHM RANKONE-002 CROSS REGION FMR	75
56	ALGORITHM RANKONE-003 CROSS REGION FMR	76
57	ALGORITHM SAMTECH-000 CROSS REGION FMR	77
58	ALGORITHM SHAMAN-000 CROSS REGION FMR	78
59	ALGORITHM SHAMAN-001 CROSS REGION FMR	79
60	ALGORITHM TEVIAN-000 CROSS REGION FMR	80
61	ALGORITHM TONGYITRANS-001 CROSS REGION FMR	81
62	ALGORITHM TONGYITRANS-002 CROSS REGION FMR	82
63	ALGORITHM TOSHIBA-000 CROSS REGION FMR	83
64	ALGORITHM TOSHIBA-001 CROSS REGION FMR	84
65	ALGORITHM ULTINOUS-000 CROSS REGION FMR	85

66	ALGORITHM VCOG-002 CROSS REGION FMR	86
67	ALGORITHM VIGILANTSOLUTIONS-002 CROSS REGION FMR	87
68	ALGORITHM VIGILANTSOLUTIONS-003 CROSS REGION FMR	88
69	ALGORITHM VISIONLABS-001 CROSS REGION FMR	89
70	ALGORITHM VISIONLABS-002 CROSS REGION FMR	90
71	ALGORITHM VOCORD-002 CROSS REGION FMR	91
72	ALGORITHM YISHENG-000 CROSS REGION FMR	92
73	ALGORITHM YISHENG-001 CROSS REGION FMR	93
74	ALGORITHM YITU-000 CROSS REGION FMR	94
75	ALGORITHM 3DIVI-001 CROSS COUNTRY FMR	95
76	ALGORITHM 3DIVI-002 CROSS COUNTRY FMR	96
77	ALGORITHM AWARE-000 CROSS COUNTRY FMR	97
78	ALGORITHM AWARE-001 CROSS COUNTRY FMR	98
79	ALGORITHM AYONIX-000 CROSS COUNTRY FMR	99
80	ALGORITHM CAMVI-001 CROSS COUNTRY FMR	100
81	ALGORITHM COGENT-000 CROSS COUNTRY FMR	101
82	ALGORITHM CYBEREXTRUDER-001 CROSS COUNTRY FMR	102
83	ALGORITHM DERMALOG-003 CROSS COUNTRY FMR	103
84	ALGORITHM DERMALOG-004 CROSS COUNTRY FMR	104
85	ALGORITHM DIGITALBARRIERS-000 CROSS COUNTRY FMR	105
86	ALGORITHM DIGITALBARRIERS-001 CROSS COUNTRY FMR	106
87	ALGORITHM FDU-000 CROSS COUNTRY FMR	107
88	ALGORITHM ID3-001 CROSS COUNTRY FMR	108
89	ALGORITHM ID3-002 CROSS COUNTRY FMR	109
90	ALGORITHM INNOVATRICES-000 CROSS COUNTRY FMR	110
91	ALGORITHM INNOVATRICES-001 CROSS COUNTRY FMR	111
92	ALGORITHM INTELLIVISION-001 CROSS COUNTRY FMR	112
93	ALGORITHM ISITYOU-000 CROSS COUNTRY FMR	113
94	ALGORITHM ISYSTEMS-000 CROSS COUNTRY FMR	114
95	ALGORITHM ITMO-002 CROSS COUNTRY FMR	115
96	ALGORITHM MORPHO-000 CROSS COUNTRY FMR	116
97	ALGORITHM MORPHO-002 CROSS COUNTRY FMR	117
98	ALGORITHM NEUROTECHNOLOGY-001 CROSS COUNTRY FMR	118
99	ALGORITHM NEUROTECHNOLOGY-002 CROSS COUNTRY FMR	119
100	ALGORITHM NOBLIS-000 CROSS COUNTRY FMR	120
101	ALGORITHM NTECHLAB-002 CROSS COUNTRY FMR	121
102	ALGORITHM NTECHLAB-003 CROSS COUNTRY FMR	122
103	ALGORITHM PA-002 CROSS COUNTRY FMR	123
104	ALGORITHM RANKONE-002 CROSS COUNTRY FMR	124
105	ALGORITHM RANKONE-003 CROSS COUNTRY FMR	125
106	ALGORITHM SAMTECH-000 CROSS COUNTRY FMR	126
107	ALGORITHM SHAMAN-000 CROSS COUNTRY FMR	127
108	ALGORITHM SHAMAN-001 CROSS COUNTRY FMR	128
109	ALGORITHM TEVIAN-000 CROSS COUNTRY FMR	129
110	ALGORITHM TONGYITRANS-001 CROSS COUNTRY FMR	130
111	ALGORITHM TONGYITRANS-002 CROSS COUNTRY FMR	131
112	ALGORITHM TOSHIBA-000 CROSS COUNTRY FMR	132
113	ALGORITHM TOSHIBA-001 CROSS COUNTRY FMR	133
114	ALGORITHM ULTINOUS-000 CROSS COUNTRY FMR	134
115	ALGORITHM VCOG-002 CROSS COUNTRY FMR	135
116	ALGORITHM VIGILANTSOLUTIONS-002 CROSS COUNTRY FMR	136
117	ALGORITHM VISIONLABS-001 CROSS COUNTRY FMR	137
118	ALGORITHM VISIONLABS-002 CROSS COUNTRY FMR	138
119	ALGORITHM VOCORD-002 CROSS COUNTRY FMR	139
120	ALGORITHM YISHENG-000 CROSS COUNTRY FMR	140
121	ALGORITHM YISHENG-001 CROSS COUNTRY FMR	141
122	ALGORITHM YITU-000 CROSS COUNTRY FMR	142

123	IMPOSTOR COUNTS FOR CROSS COUNTRY FMR CALCULATIONS	143
124	ALGORITHM 3DIVI-001 CROSS AGE FMR	145
125	ALGORITHM 3DIVI-002 CROSS AGE FMR	146
126	ALGORITHM AWARE-000 CROSS AGE FMR	147
127	ALGORITHM AWARE-001 CROSS AGE FMR	148
128	ALGORITHM AYONIX-000 CROSS AGE FMR	149
129	ALGORITHM CAMVI-001 CROSS AGE FMR	150
130	ALGORITHM COGENT-000 CROSS AGE FMR	151
131	ALGORITHM CYBEREXTRUDER-001 CROSS AGE FMR	152
132	ALGORITHM DERMALOG-003 CROSS AGE FMR	153
133	ALGORITHM DERMALOG-004 CROSS AGE FMR	154
134	ALGORITHM DIGITALBARRIERS-000 CROSS AGE FMR	155
135	ALGORITHM DIGITALBARRIERS-001 CROSS AGE FMR	156
136	ALGORITHM FDU-000 CROSS AGE FMR	157
137	ALGORITHM FDU-001 CROSS AGE FMR	158
138	ALGORITHM ID3-001 CROSS AGE FMR	159
139	ALGORITHM ID3-002 CROSS AGE FMR	160
140	ALGORITHM INNOVATRICES-000 CROSS AGE FMR	161
141	ALGORITHM INNOVATRICES-001 CROSS AGE FMR	162
142	ALGORITHM INTELLIVISION-001 CROSS AGE FMR	163
143	ALGORITHM ISITYOU-000 CROSS AGE FMR	164
144	ALGORITHM ISYSTEMS-000 CROSS AGE FMR	165
145	ALGORITHM ITMO-002 CROSS AGE FMR	166
146	ALGORITHM MORPHO-000 CROSS AGE FMR	167
147	ALGORITHM MORPHO-002 CROSS AGE FMR	168
148	ALGORITHM NEUROTECHNOLOGY-001 CROSS AGE FMR	169
149	ALGORITHM NEUROTECHNOLOGY-002 CROSS AGE FMR	170
150	ALGORITHM NOBLIS-000 CROSS AGE FMR	171
151	ALGORITHM NTECHLAB-002 CROSS AGE FMR	172
152	ALGORITHM NTECHLAB-003 CROSS AGE FMR	173
153	ALGORITHM PA-002 CROSS AGE FMR	174
154	ALGORITHM RANKONE-002 CROSS AGE FMR	175
155	ALGORITHM RANKONE-003 CROSS AGE FMR	176
156	ALGORITHM SAMTECH-000 CROSS AGE FMR	177
157	ALGORITHM SHAMAN-000 CROSS AGE FMR	178
158	ALGORITHM SHAMAN-001 CROSS AGE FMR	179
159	ALGORITHM TEVIAN-000 CROSS AGE FMR	180
160	ALGORITHM TONGYITRANS-001 CROSS AGE FMR	181
161	ALGORITHM TONGYITRANS-002 CROSS AGE FMR	182
162	ALGORITHM TOSHIBA-000 CROSS AGE FMR	183
163	ALGORITHM TOSHIBA-001 CROSS AGE FMR	184
164	ALGORITHM ULTINOUS-000 CROSS AGE FMR	185
165	ALGORITHM VCOG-002 CROSS AGE FMR	186
166	ALGORITHM VIGILANTSOLUTIONS-002 CROSS AGE FMR	187
167	ALGORITHM VIGILANTSOLUTIONS-003 CROSS AGE FMR	188
168	ALGORITHM VISIONLABS-001 CROSS AGE FMR	189
169	ALGORITHM VISIONLABS-002 CROSS AGE FMR	190
170	ALGORITHM VOCORD-002 CROSS AGE FMR	191
171	ALGORITHM YISHENG-000 CROSS AGE FMR	192
172	ALGORITHM YISHENG-001 CROSS AGE FMR	193
173	ALGORITHM YITU-000 CROSS AGE FMR	194

1 News

2017-01-05

- ▷ NIST's evaluation of 1:N identification algorithms starts January 22, with algorithm submission deadline February 16.
- ▷ NIST's evaluation of 1:1 algorithms will close starting February 12, and will resume in May.
- ▷ The 1:N test will use N well in excess of 10^7 .
- ▷ The 1:N API and concept document is linked from [here](#).

2 Changelog

2018-01-24

- ▷ Added results for first algorithms from Gemalto Cogent, Intellivision and Ultinuous.
- ▷ Added full or partial results for new algorithms from Idemia (Morpho), NTechLab, Shaman, Tevian, and Toshiba, and from Fudan and ITMO universities.
- ▷ Added entries for Fudan University which had incorrectly been omitted from Tables 1 and 3.
- ▷ Retired results for itmo-001, ntechlab-001, vocord-001, and vigilantsolutions-001 - FRVT lists only the two most recent algorithms per organization.
- ▷ Added GPU vs CPU shape designators to the tradeoff summaries in Figures 1 and 2.
- ▷ We expect to produce another edition of this FRVT report on February 13.

2017-12-14

- ▷ Added results for algorithms from Aware, RankOne, Shaman, and Tevian.
- ▷ Retired results for RankOne-000 - FRVT lists only the two most recent algorithms per organization.
- ▷ New description of wild images in section 5.2
- ▷ New Figure 23 showing FMR for impostors of same age, sex and worst-case region.

2017-11-16

- ▷ Added results for algorithms from 3DiVi, Dermalog, Neurotechnology and Ping An.
- ▷ Retired results for 3DiVi-000, dermalog-002, and neurotechnology-000 - FRVT lists only two algorithms per organization.
- ▷ Retired results for vcognition-001 as the algorithm was inoperable on at least one dataset.
- ▷ Added cross-pose recognition heatmaps for the wild images, Figures 10 and 11.
- ▷ Added Figure 14 to compare effect of providing whole vs. face-cropped child exploitation images.

2017-10-03

- ▷ Added results for algorithms from 3DiVi, Camvi, Idemia, Noblis, N-TechLab, and Visionlabs.
- ▷ Added partial results for two algorithms from Zhuhai Yisheng.
- ▷ The ntechlab-000 algorithm has been retired - FRVT lists only two algorithms per organization.
- ▷ Corrected fixed FMR operating point in the legends of some DET plots.

2017-08-22

- ▷ Added results for three additional algorithms, rankone-002, neurotechnology-001, and itmo-002.
- ▷ The algorithms dermalog-001 and rank-001 have been retired - FRVT lists only two algorithms per organization
- ▷ The algorithm tupel-001 has been retired as it is not operable on all datasets
- ▷ Clarified the tradeoff Figures 1 and 2 plot only genuine comparison durations.
- ▷ Corrected image type label in section 4.5

2017-08-07

- ▷ Added results for 5 new algorithms
- ▷ Added Figure 3 giving simulated example images.
- ▷ Added Figure 1 showing an alternative view of the same tradeoff data in Figure 2
- ▷ Added Figure 5 showing accuracy on visa images just for low FMR.
- ▷ Added Figure 24 showing impostor distribution shifts from certain country pairs. Section 5.6.1 in this and prior reports documents high false match rates for individuals from certain countries. That effect, however, is often not confined to anomalously high impostor scores in the tails of the distribution, but arises from systematic shifts of the whole distribution. These shifts sometimes reach 2σ .

2017-07-29

- ▷ Added results for 8 new algorithms
- ▷ Added results for a child-exploitation dataset
- ▷ Added Table 2 a standalone tabulation of false non-match rates
- ▷ We have received additional CPU algorithms - Results should appear August 4, 2017
- ▷ We have received additional GPU algorithms - Results to appear as computational resources are released from the Face Recognition Prize Challenge

2017-06-19

- ▷ Added five new algorithms, three of which remain in-process
- ▷ Added results for a “wild” dataset of images similar to non-cooperative photojournalism images
- ▷ Added Table 3 a standalone tabulation of failure to enrol rates
- ▷ Added Fig. 2 showing tradeoff between FNMR, template size, template generation time, and match duration.
- ▷ Added Fig. 19 showing how FMR is concentrated in certain images.
- ▷ Restated cross-region false match rates at nominal FMR = 0.0001 instead of 0.001
- ▷ Improved DET legends.

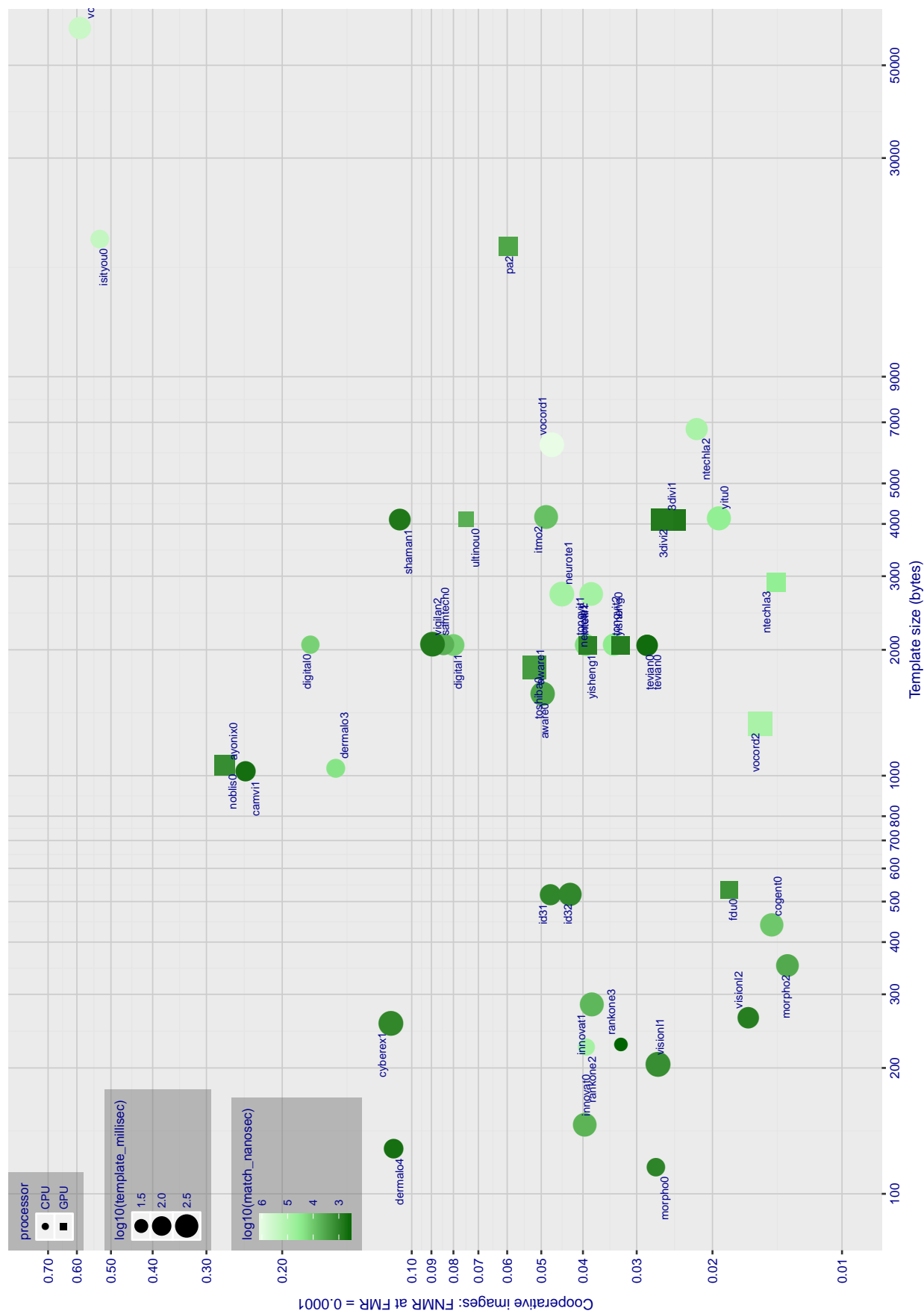
	Developer	Short	Seq.	Validation	Config ¹	Template		GPU	Comparison Time (ns) ³	
	Name	Name	Num.	Date	Data (KB)	Size (B)	Time (ms) ²		Genuine	Impostor
1	3DiVi	3divi	001	2017-06-22	190867	⁴⁰ 4096 ± 0	²³ 274 ± 47	Yes	¹⁰ 636 ± 19	¹⁰ 634 ± 16
2	3DiVi	3divi	002	2017-10-20	190867	⁴² 4096 ± 0	²⁴ 279 ± 48	Yes	¹² 692 ± 22	¹³ 707 ± 26
3	Aware	aware	000	2017-10-27	240240	²² 1572 ± 0	⁴¹ 655 ± 26	No	²⁹ 4030 ± 83	²⁹ 2984 ± 152
4	Aware	aware	001	2017-10-27	240240	²³ 1572 ± 0	⁴² 656 ± 26	No	²⁶ 2902 ± 51	²⁷ 2810 ± 111
5	Ayonix	ayonix	000	2017-06-22	58505	¹⁷ 1036 ± 0	¹ 18 ± 2	No	⁷ 621 ± 23	⁹ 620 ± 26
6	Camvi Technologies	camvitech	001	2017-09-13	118759	¹⁶ 1024 ± 0	¹⁵ 181 ± 6	No	⁵ 481 ± 16	⁸ 487 ± 23
7	Gemalto Cogent	cogent	000	2018-01-12	633812	¹¹ 439 ± 0	³³ 511 ± 7	No	³⁵ 9541 ± 54	³⁶ 9500 ± 51
8	Cyberextruder	cyberex	001	2017-08-02	121211	⁷ 256 ± 0	⁴⁸ 893 ± 25	No	¹⁸ 1083 ± 16	²⁰ 1079 ± 19
9	Dermalog	dermalog	003	2017-07-10	0	¹⁸ 1043 ± 0	¹² 121 ± 22	No	³⁹ 22957 ± 93	⁴¹ 22808 ± 131
10	Dermalog	dermalog	004	2017-10-26	0	² 128 ± 0	¹⁵ 149 ± 5	No	⁶ 490 ± 26	⁷ 471 ± 26
11	Digital Barriers	barriers	000	2017-05-31	157794	²⁸ 2056 ± 0	⁹ 104 ± 0	No	³⁷ 13232 ± 166	³⁸ 13226 ± 146
12	Digital Barriers	barriers	001	2017-07-20	236915	³⁰ 2056 ± 0	²⁵ 294 ± 1	No	³⁶ 12311 ± 164	³⁷ 12347 ± 197
13	Fudan University	fudan	000	2017-11-22	202296	¹⁴ 534 ± 0	⁶ 84 ± 0	Yes	²² 1713 ± 28	²³ 1715 ± 20
14	ID3 Technology	id3	001	2017-08-04	225574	¹³ 520 ± 0	¹⁹ 238 ± 19	No	¹⁷ 1058 ± 32	¹⁹ 1049 ± 28
15	ID3 Technology	id3	002	2017-08-04	225574	¹² 520 ± 0	³² 482 ± 34	No	¹⁹ 1100 ± 59	¹⁸ 1048 ± 32
16	Innovatrics	innova	000	2017-07-25	0	³ 146 ± 0	³⁵ 578 ± 5	No	³² 4964 ± 63	³³ 4665 ± 262
17	Innovatrics	innova	001	2017-07-25	0	⁹ 284 ± 0	³⁹ 645 ± 5	No	³³ 5506 ± 131	³⁴ 4975 ± 308
18	Intellivision	intellivision	001	2017-10-10	43692	³¹ 2056 ± 0	⁴ 62 ± 2	No	²⁴ 2573 ± 91	²⁶ 2544 ± 38
19	Is It You	isityou	000	2017-06-26	48010	⁴⁸ 19200 ± 0	¹¹ 113 ± 5	No	⁴⁸ 237517 ± 1318	⁴⁸ 237374 ± 1279
20	Innovation Systems	isystems	000	2018-01-11	209270	¹⁵ 1024 ± 0	¹⁶ 154 ± 4	No	³ 398 ± 14	⁴ 396 ± 16
21	ITMO University	itmo	002	2017-08-07	1923215	⁴⁵ 4162 ± 0	³⁷ 611 ± 17	No	³⁴ 7423 ± 96	³⁵ 7451 ± 94
22	Idemia	morpho	000	2017-07-11	100806	¹ 116 ± 0	¹⁰ 109 ± 1	No	¹⁶ 993 ± 31	¹⁷ 1000 ± 34
23	Idemia	morpho	002	2017-12-28	383021	¹⁰ 352 ± 0	³¹ 411 ± 7	No	²⁸ 3620 ± 94	²⁵ 2481 ± 65
24	Neurotechnology	neurotech	001	2017-08-07	280771	³⁶ 2718 ± 0	⁴⁷ 881 ± 46	No	⁴⁵ 69356 ± 684	⁴⁵ 69140 ± 579
25	Neurotechnology	neurotech	002	2017-11-02	280771	³⁷ 2718 ± 0	³⁶ 581 ± 6	No	⁴³ 68738 ± 748	⁴⁴ 68905 ± 993
26	Noblis	noblis	000	2017-07-05	713573	¹⁹ 1061 ± 0	¹⁷ 174 ± 20	Yes	²⁰ 1343 ± 45	²² 1373 ± 56
27	N-Tech Lab	ntech	002	2017-08-23	894169	⁴⁶ 6744 ± 1	²⁸ 330 ± 11	No	⁴⁶ 82508 ± 213	⁴⁶ 82524 ± 220
28	N-Tech Lab	ntech	003	2017-12-29	1422738	³⁸ 2906 ± 1	¹³ 128 ± 3	Yes	⁴¹ 35327 ± 117	⁴² 35371 ± 123
29	Ping An Technology	Pingan	002	2017-09-25	442564	⁴⁷ 18436 ± 0	¹⁴ 132 ± 7	Yes	²⁷ 3088 ± 32	³⁰ 3051 ± 28
30	Rank One Computing	rankone	002	2017-08-18	0	⁵ 224 ± 0	⁵ 75 ± 1	No	⁴⁴ 69113 ± 3802	² 369 ± 26
31	Rank One Computing	rankone	003	2017-11-28	0	⁶ 228 ± 0	² 37 ± 1	No	¹ 322 ± 20	¹ 324 ± 19
32	Samtech InfoNet Limited	samtech	000	2017-05-02	109774	²⁹ 2056 ± 0	²¹ 262 ± 2	No	³¹ 4550 ± 26	³² 4541 ± 28
33	Shaman Software	shaman	000	2017-12-05	0	⁴¹ 4096 ± 0	⁴⁰ 653 ± 16	No	² 380 ± 25	³ 379 ± 31
34	Shaman Software	shaman	001	2018-01-13	0	³⁹ 4096 ± 0	²⁶ 294 ± 2	No	⁹ 635 ± 19	⁶ 441 ± 25
35	Teveian	teveian	001	2018-01-19	455746	²⁷ 2048 ± 0	²⁰ 242 ± 14	No	⁴ 430 ± 38	⁵ 427 ± 23
36	TongYi Transportation Technology	tongyi	001	2017-04-01	625339	³² 2058 ± 0	²⁷ 310 ± 20	No	³⁸ 17769 ± 74	³⁹ 17750 ± 63
37	TongYi Transportation Technology	tongyi	002	2017-07-15	625336	³³ 2058 ± 0	²⁹ 356 ± 35	No	⁴⁰ 29816 ± 281	⁴⁰ 17799 ± 127
38	Toshiba	toshiba	000	2018-01-11	3893310	²⁴ 1812 ± 0	³⁴ 528 ± 3	Yes	²³ 2255 ± 60	²⁴ 2251 ± 53
39	Toshiba	toshiba	001	2018-01-11	3893310	³⁵ 2580 ± 0	³⁸ 615 ± 3	Yes	²⁵ 2900 ± 80	²⁸ 2881 ± 60
40	Ultinuous	ultinuous	000	2017-12-18	90803	⁴³ 4100 ± 0	³ 53 ± 0	Yes	³⁰ 4263 ± 50	³¹ 4262 ± 42
41	VCognition	vcog	002	2017-06-12	3229434	⁴⁹ 61504 ± 5	³⁰ 357 ± 25	No	⁴⁹ 296154 ± 3077	⁴⁹ 296436 ± 4183
42	Vigilant Solutions	vigilant	002	2017-09-28	344137	³⁴ 2060 ± 0	⁴⁶ 844 ± 2	No	¹¹ 679 ± 10	¹² 680 ± 7
43	Vigilant Solutions	vigilant	003	2018-01-23	343048	²¹ 1548 ± 0	⁴⁵ 824 ± 3	No	⁸ 634 ± 19	¹¹ 638 ± 17
44	VisionLabs	visionlabs	001	2017-06-12	343661	⁴ 204 ± 0	⁴⁹ 943 ± 8	No	²¹ 1395 ± 45	²¹ 1148 ± 53
45	VisionLabs	visionlabs	002	2017-09-08	591936	⁸ 264 ± 0	²² 265 ± 8	No	¹⁴ 796 ± 35	¹⁵ 799 ± 31
46	Vocord	vocord	002	2017-06-07	918292	²⁰ 1330 ± 0	⁴⁷ 82 ± 36	Yes	⁴⁷ 83063 ± 517	⁴⁷ 83072 ± 714
47	Zhuhai Yisheng Electronics Technology	yisheng	000	2017-08-17	122704	²⁶ 2048 ± 0	⁸ 103 ± 1	Yes	¹³ 790 ± 23	¹⁴ 789 ± 20
48	Zuhai Yisheng Electronics Technology	yisheng	001	2017-08-17	120112	²⁵ 2048 ± 0	⁷ 103 ± 1	Yes	¹⁵ 906 ± 31	¹⁶ 905 ± 25
49	Shanghai Yitu Technology	yitu	000	2017-05-23	2211068	⁴⁴ 4130 ± 0	⁴³ 672 ± 2	No	⁴² 35352 ± 114	⁴³ 37848 ± 1773

Notes	
1	The configuration size does not capture static data included in libraries. We do not count these because some algorithms include common ancilliary libraries for image processing (e.g. openCV) or numerical computation (e.g. blas).
2	The median template creation times are measured on Intel®Xeon®CPU E5-2630 v4 @ 2.20GHz processors or, for GPU-enabled implementations, NVidia Tesla K40.
3	The comparison durations, in nanoseconds, are estimated using std::chrono::high_resolution_clock which on the machine in (2) counts 1ns clock ticks. Precision is somewhat worse than that however. The ± value is the median absolute deviation times 1.48 for Normal consistency.

Table 1: Summary of algorithms and properties included in this report. The red superscripts give ranking for the quantities in that column.

	Algorithm	FALSE NON-MATCH RATE (FNMR)											
		CONSTRAINED, COOPERATIVE						LESS CONSTRAINED, NON-COOPERATIVE					
		VISA		VISA		MUGSHOT		WEBCAM		SELFIE		WILD	
	Name												
	FMR	1E-06		0.0001		0.0001		0.0001		0.0001		0.0001	0.01
1	3divi-001	0.154	17	0.020	9	0.030	16	0.001	15	0.046	26	0.492	7
2	3divi-002	0.154	16	0.021	11	0.033	19	0.001	17	0.049	30	0.495	8
3	aware-000	0.309	39	0.054	32	0.045	30	0.003	23	0.046	28	0.948	42
4	aware-001	0.309	40	0.054	31	0.045	31	0.004	25	0.046	27	0.993	45
5	ayonix-000	0.487	46	0.230	49	0.309	45	0.172	46	0.360	46	0.807	33
6	camvi-001	0.538	48	0.183	47	0.323	46	0.106	44	0.268	45	0.743	29
7	cogent-000	0.084	11	0.012	3	0.018	2	0.001	13	0.014	9	0.508	10
8	cyberextruder-001	0.255	33	0.076	37	0.165	42	0.029	38	0.144	42	0.853	36
9	dermalog-003	0.280	35	0.112	42	0.202	44	0.041	42	0.115	39	0.693	23
10	dermalog-004	0.240	31	0.093	41	0.131	41	0.016	34	0.121	41	0.996	47
11	digitalbarriers-000	0.463	45	0.161	45	0.184	43	0.045	43	0.170	43	0.741	28
12	digitalbarriers-001	0.502	47	0.155	44	0.041	26	0.029	39	0.115	38	0.678	21
13	fdi-000	0.058	6	0.016	6	0.021	8	0.001	12	0.009	3	0.549	11
14	fdi-001	0.044	4	0.017	7	0.024	12	-	52	-	52	-	52
15	id3-001	0.250	32	0.063	34	0.036	20	0.002	20	0.040	21	0.765	30
16	id3-002	0.239	30	0.057	33	0.032	18	0.003	24	0.037	16	0.810	34
17	innovatrics-000	0.191	24	0.034	20	0.046	33	0.001	11	0.040	18	0.720	26
18	innovatrics-001	0.183	22	0.034	19	0.043	28	0.001	14	0.043	22	0.643	17
19	intellivision-001	0.221	28	0.042	26	0.037	21	0.021	37	0.066	35	0.878	38
20	isityou-000	0.703	50	0.414	50	0.680	49	0.690	48	-	49	1.000	48
21	isystems-000	0.179	20	0.043	27	0.064	37	0.008	28	0.049	29	0.678	20
22	itmo-002	0.287	37	0.050	30	0.047	34	0.036	41	0.069	36	0.892	40
23	itmo-003	0.140	15	0.020	8	-	52	-	50	-	50	-	49
24	morpho-000	0.134	14	0.026	13	0.028	14	0.007	27	0.012	6	0.893	41
25	morpho-002	0.068	9	0.009	1	0.019	5	0.000	4	0.006	2	0.607	14
26	neurotechnology-001	0.222	29	0.044	28	0.046	32	0.001	16	0.017	12	0.817	35
27	neurotechnology-002	0.166	19	0.036	21	0.041	25	0.000	6	0.020	14	0.427	4
28	noblis-000	0.542	49	0.212	48	0.349	47	0.153	45	0.239	44	0.875	37
29	ntechlab-002	0.065	7	0.021	10	0.023	10	0.003	21	0.014	8	0.324	2
30	ntechlab-003	0.039	3	0.011	2	0.019	4	0.003	22	0.014	10	0.271	1
31	pa-002	0.286	36	0.086	39	0.041	27	0.010	30	0.043	24	0.633	16
32	rankone-002	0.217	27	0.049	29	0.032	17	0.000	7	0.052	31	0.705	25
33	rankone-003	0.184	23	0.038	25	0.028	13	0.000	5	0.040	19	0.674	18
34	samtech-000	0.443	43	0.161	46	0.044	29	0.021	36	0.063	34	0.878	39
35	shaman-000	0.977	52	0.913	52	0.968	51	0.992	49	0.997	48	0.995	46
36	shaman-001	0.462	44	0.136	43	0.083	39	0.030	40	0.115	40	0.775	31
37	tevia-000	0.129	13	0.036	22	0.022	9	0.002	19	0.009	4	0.500	9
38	tevia-001	0.127	12	0.033	18	0.021	7	0.002	18	0.006	1	0.448	6
39	tiger-001	-	53	-	53	0.398	48	0.015	33	0.046	25	-	50
40	tongyitrans-001	0.072	10	0.038	24	0.041	24	0.009	29	0.063	32	0.704	24
41	tongyitrans-002	0.066	8	0.030	14	0.039	22	0.010	31	0.063	33	0.725	27
42	toshiba-000	0.290	38	0.069	36	0.039	23	-	53	-	53	-	53
43	toshiba-001	0.193	25	0.033	17	-	53	-	51	-	51	-	51
44	ultinuous-000	0.348	42	0.076	38	0.073	38	0.005	26	0.040	20	0.979	44
45	vcog-002	0.903	51	0.504	51	0.692	50	0.559	47	0.666	47	0.778	32
46	vigilantsolutions-002	0.321	41	0.087	40	0.092	40	0.018	35	0.075	37	0.675	19
47	vigilantsolutions-003	0.267	34	0.068	35	0.057	36	0.001	9	0.037	17	0.571	12
48	visionlabs-001	0.180	21	0.030	15	0.024	11	0.001	8	0.014	11	0.591	13
49	visionlabs-002	0.051	5	0.014	5	0.020	6	0.001	10	0.017	13	0.397	3
50	vocord-002	0.034	2	0.013	4	0.019	3	0.011	32	0.012	7	0.948	43
51	yisheng-000	0.199	26	0.037	23	0.029	15	0.000	2	0.035	15	0.686	22
52	yisheng-001	0.160	18	0.032	16	0.048	35	0.000	3	0.043	23	0.628	15
53	yitu-000	0.033	1	0.021	12	0.017	1	0.000	1	0.012	5	0.431	5

Table 2: FNMR is the proportion of mated comparisons below a threshold set to achieve the FMR given in the header on the fourth row. FMR is the proportion of impostor comparisons at or above that threshold. Note that the webcam and selfie values apply to images collected on the same day, and that will often yield optimistically low FNMR values.



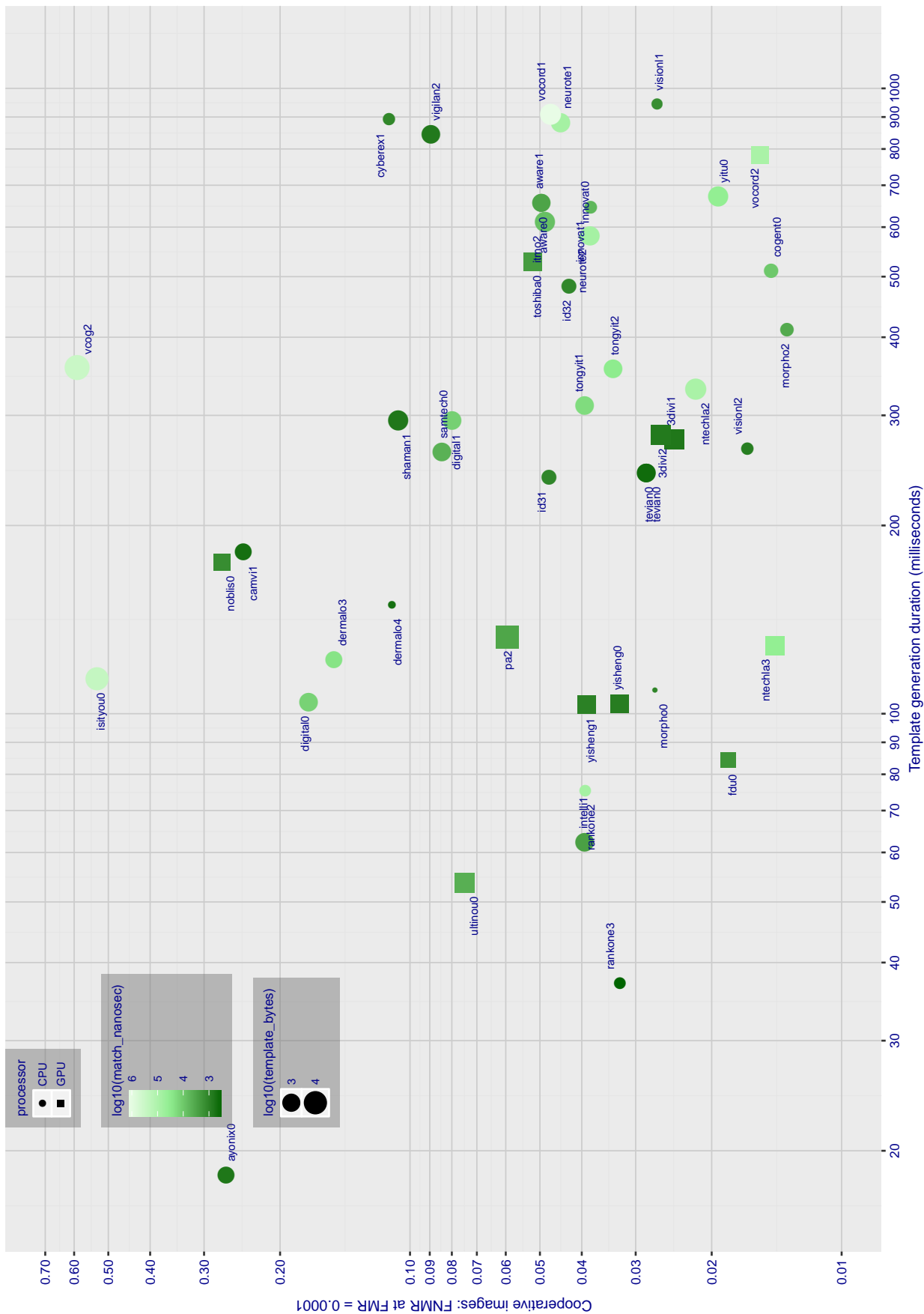


Figure 2: The points show false non-match rates (FNMR) versus the duration of the template generation operation. Some algorithms run on GPU, most on CPU - see Table 1. FNMR is the geometric mean of FNMR values for visa and mugshot images (from Figs. 4 and 6) at a false match rate (FMR) of 0.0001. Template generation time is a median estimated over 640 x 480 pixel portraits. The size of the points encodes template size - which span two orders of magnitude. The color of the points encodes one-to-one genuine template comparison duration - which span three orders of magnitude.

3 Metrics

3.1 Core accuracy

Given a vector of N genuine scores, u , the false non-match rate (FNMR) is computed as the proportion below some threshold, T :

$$\text{FNMR}(T) = 1 - \frac{1}{N} \sum_{i=1}^N H(u_i - T) \quad (1)$$

where $H(x)$ is the unit step function, and $H(0)$ taken to be 1.

Similarly, given a vector of N impostor scores, v , the false match rate (FMR) is computed as the proportion above T :

$$\text{FMR}(T) = \frac{1}{N} \sum_{i=1}^N H(v_i - T) \quad (2)$$

The threshold, T , can take on any value. We typically generate a set of thresholds from quantiles of the observed impostor scores, v , as follows. Given some interesting false match rate range, $[\text{FMR}_L, \text{FMR}_U]$, we form a vector of K thresholds corresponding to FMR measurements evenly spaced on a logarithmic scale

$$T_k = Q_v(1 - \text{FMR}_k) \quad (3)$$

where Q is the quantile function, and FMR_k comes from

$$\log_{10} \text{FMR}_k = \log_{10} \text{FMR}_L + \frac{k}{K} [\log_{10} \text{FMR}_U - \log_{10} \text{FMR}_L] \quad (4)$$

Error tradeoff characteristics are plots of $\text{FNMR}(T)$ vs. $\text{FMR}(T)$. These are plotted with $\text{FMR}_U \rightarrow 1$ and FMR_L as low as is sustained by the number of impostor comparisons, N . This is somewhat higher than the “rule of three” limit $3/N$ because samples are not independent, due to re-use of images.

4 Datasets

4.1 Child exploitation images

- ▷ The number of images is $O(10^4)$.
- ▷ The number of subjects is $O(10^3)$.
- ▷ The number of subjects with two images $O(10^3)$.
- ▷ The images are operational. They are taken from ongoing investigations of child exploitation crimes. The images are arbitrarily unconstrained. Pose varies considerably around all three axes, including subject lying down. Resolution varies very widely. Faces can be occluded by other objects, including hair and hands. Lighting varies, although the images are intended for human viewing. Mis-focus is rare. Images are given to the algorithm without any cropping; faces may occupy widely varying areas.
- ▷ The images are usually large from contemporary cameras. The mean interocular distance (IOD) is 70 pixels.
- ▷ The images are of subjects from several countries, due to the global production of this imagery.
- ▷ The images are of children, from infancy to late adolescence.
- ▷ All of the images are live capture, none are scanned. Many have been cropped.
- ▷ When these images are input to the algorithm, they are labelled as being of type "EXPLOITATION" - see Table 4 of the FRVT API.

4.2 Visa images

- ▷ The number of images is $O(10^5)$.
- ▷ The number of subjects is $O(10^5)$.
- ▷ The number of subjects with two images $O(10^4)$.
- ▷ The images have geometry in reasonable conformance with the ISO/IEC 19794-5 Full Frontal image type. Pose is generally excellent.
- ▷ The images are of size 252x300 pixels. The mean interocular distance (IOD) is 69 pixels.
- ▷ The images are of subjects from greater than 100 countries, with significant imbalance due to visa issuance patterns.
- ▷ The images are of subjects of all ages, including children, again with imbalance due to visa issuance demand.
- ▷ Many of the images are live capture. A substantial number of the images are photographs of paper photographs.
- ▷ When these images are input to the algorithm, they are labelled as being of type "ISO" - see Table 4 of the FRVT API.

4.3 Mugshot images

- ▷ The number of images is $O(10^6)$.
- ▷ The number of subjects is $O(10^5)$.
- ▷ The number of subjects with two images $O(10^5)$.

- ▷ The images have geometry in reasonable conformance with the ISO/IEC 19794-5 Full Frontal image type.
- ▷ The images are of variable sizes. The median IOD is 104 pixels. The mean IOD is 123 pixels.
- ▷ The images are of subjects from the United States.
- ▷ The images are of adults.
- ▷ The images are all live capture.
- ▷ When these images are input to the algorithm, they are labelled as being of type "mugshot" - see Table 4 of the FRVT API.

4.4 Selfie images

- ▷ The number of images is below 500.
- ▷ The number of subjects is below 500.
- ▷ All subjects have a selfie image, and a portrait image.
- ▷ The portrait images are in reasonable conformance with the ISO/IEC 19794-5 Full Frontal image type.
- ▷ The selfie images vary: taken with camera above and below eye level, with one hand or two hands. Pitch angles vary more than yaw angles, which are frontal. Some perspective distortion is evident.
- ▷ The images have mean IOD of 140 pixels.
- ▷ The images are of subjects from the United States.
- ▷ The images are of adults.
- ▷ The images are all live capture.
- ▷ When these images are input to the algorithm, they are labelled as being of type "WILD" - see Table 4 of the FRVT API.

4.5 Webcam images

- ▷ The number of images is below 1500.
- ▷ The number of subjects is below 1500.
- ▷ All subjects have a webcam image, and a portrait image.
- ▷ The portrait images are in reasonable conformance with the ISO/IEC 19794-5 Full Frontal image type.
- ▷ The webcam images are taken with camera at a typical head height, with mild pitch angles, low yaw angles, but some variation in range, such that low perspective distortion is sometimes evident.
- ▷ The images have mean IOD of 68 pixels (sd=12).
- ▷ The images are of subjects from the United States.
- ▷ The images are of adults.
- ▷ The images are all live capture.
- ▷ When these images are input to the algorithm, they are labelled as being of type "MUGSHOT" - see Table 4 of the FRVT API.

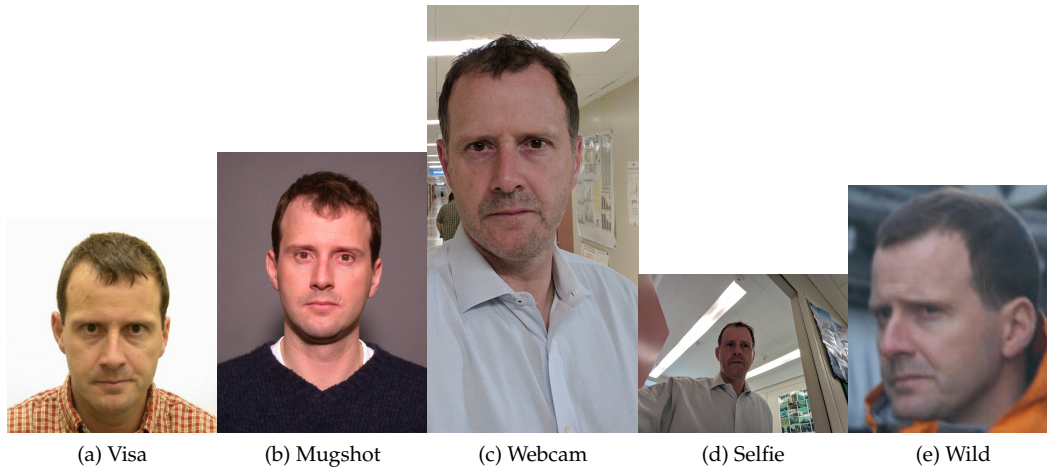


Figure 3: The figure gives simulated samples of image types used in this report.

4.6 Wild images

- ▷ The number of images is $O(10^5)$.
- ▷ The number of subjects is $O(10^3)$.
- ▷ The number of subjects with two images $O(10^3)$.
- ▷ The images include many photojournalism-style images. Images are given to the algorithm using a variable but generally tight crop of the head. Resolution varies very widely. The images are very unconstrained, with wide yaw and pitch pose variation. Faces can be occluded, including hair and hands.
- ▷ The images are of adults.
- ▷ All of the images are live capture, none are scanned.
- ▷ When these images are input to the algorithm, they are labelled as being of type "WILD" - see Table 4 of the FRVT API.

5 Results

5.1 Test goals

- ▷ To state overall accuracy.
- ▷ To compare algorithms.

5.2 Test design

Method: For wild images:

- ▷ The comparisons are of wild photos against wild photos.
- ▷ The number of genuine comparisons is $O(10^6)$.
- ▷ The number of impostor comparisons is $O(10^7)$.

- ▷ The comparisons are fully zero-effort, meaning impostors are paired without attention to sex, age or other covariates.
- ▷ The number of persons is $O(10^4)$.
- ▷ The number of images used to make 1 template is 1.
- ▷ The number of templates used to make each comparison score is two corresponding to simple one-to-one verification.

Method: For visa images:

- ▷ The comparisons are of visa photos against visa photos.
- ▷ The number of genuine comparisons is $O(10^4)$.
- ▷ The number of impostor comparisons is $O(10^{10})$.
- ▷ The comparisons are fully zero-effort, meaning impostors are paired without attention to sex, age or other covariates. However, later analysis is conducted on subsets.
- ▷ The number of persons is $O(10^5)$.
- ▷ The number of images used to make 1 template is 1.
- ▷ The number of templates used to make each comparison score is two corresponding to simple one-to-one verification.

For mugshot images:

- ▷ The comparisons are of mugshot photos against mugshot photos.
- ▷ The number of genuine comparisons is $O(10^5)$.
- ▷ The number of impostor comparisons is $O(10^7)$.
- ▷ The comparisons are fully zero-effort, meaning impostors are paired without attention to sex, age or other covariates.
- ▷ The number of persons is $O(10^6)$.
- ▷ The number of images used to make 1 template is 1.
- ▷ The number of templates used to make each comparison score is two corresponding to simple one-to-one verification.

For selfie images:

- ▷ The comparisons are of selfie photos against portrait photos.
- ▷ The number of genuine comparisons is $O(10^2)$.
- ▷ The number of impostor comparisons is $O(10^8)$ selfies are compared with portraits of $O(10^6)$ other subjects.
- ▷ The comparisons are fully zero-effort, meaning impostors are paired without attention to sex, age or other covariates.
- ▷ The number of persons is $O(10^6)$.
- ▷ The number of images used to make 1 template is 1.

- ▷ The number of templates used to make each comparison score is two corresponding to simple one-to-one verification.

For webcam images:

- ▷ The comparisons are of webcam photos against portrait photos.
- ▷ The number of genuine comparisons is $O(10^3)$.
- ▷ The number of impostor comparisons is $O(10^9)$ webcams are compared with portraits of $O(10^6)$ other subjects.
- ▷ The comparisons are fully zero-effort, meaning impostors are paired without attention to sex, age or other covariates.
- ▷ The number of persons is $O(10^6)$.
- ▷ The number of images used to make 1 template is 1.
- ▷ The number of templates used to make each comparison score is two corresponding to simple one-to-one verification.

For child exploitation images:

- ▷ The comparisons are of unconstrained child exploitation photos against others of the same type.
- ▷ The number of genuine comparisons is $O(10^4)$.
- ▷ The number of impostor comparisons is $O(10^7)$.
- ▷ The comparisons are fully zero-effort, meaning impostors are paired without attention to sex, age or other covariates.
- ▷ The number of persons is $O(10^3)$.
- ▷ The number of images used to make 1 template is 1.
- ▷ The number of templates used to make each comparison score is two corresponding to simple one-to-one verification.
- ▷ We produce two performance statements. First, is a DET as used for visa and mugshot images. The second is a cumulative match characteristic (CMC) summarizing a simulated one-to-many search process. This is done as follows.
 - We regard M enrollment templates as items in a gallery.
 - These M templates come from $M > N$ individuals, because multiple images of a subject are present in the gallery under separate identifiers.
 - We regard the verification templates as search templates.
 - For each search we compute the rank of the highest scoring mate.
 - This process should properly be conducted with a 1:N algorithm, such as those tested in NIST IR 8009. We use the 1:1 algorithms in a simulated 1:N mode here to a) better reflect what a child exploitation analyst does, and b) to do show algorithm efficacy is better than that revealed in the verification DETs.

5.3 Failure to enrol

Algorithm Name	Failure to Enrol Rate ¹									
	CHILD-EXPLOIT		MUGSHOT		SELFIES		VISA		WEBCAM	
3divi-001	0.2006	21	0.0019	34	0.0202	33	0.0007	27	0.0020	21
3divi-002	0.3103	29	0.0039	44	0.0376	40	0.0010	30	0.0027	32
aware-000	0.4663	43	0.0018	33	0.0231	35	0.0005	21	0.0055	37
aware-001	0.1897	20	0.0010	20	0.0145	30	0.0002	12	0.0048	36
ayonix-000	0.0000	3	0.0109	53	0.0751	48	0.0137	57	0.0109	41
camvi-001	0.3931	40	0.0033	42	0.0231	36	0.0010	33	0.0027	33
cogent-000	0.2914	26	0.0011	22	0.0029	15	0.0005	23	0.0020	28
cyberextruder-001	0.5338	49	0.0036	43	0.0376	39	0.0029	45	0.0205	45
dermalog-003	0.0434	11	0.0007	14	0.0000	2	0.0025	43	0.0007	11
dermalog-004	0.3110	30	0.0031	41	0.0087	25	0.0090	55	0.0020	27
digitalbarriers-000	0.5469	50	0.0043	46	0.0925	49	0.0019	41	0.0184	44
digitalbarriers-001	0.5102	48	0.0044	47	0.0925	50	0.0018	40	0.0232	46
fdi-000	0.4992	47	0.0025	38	0.0029	19	0.0011	35	0.0020	30
fdi-001	0.1380	19	0.0015	28	-	49	0.0009	29	-	49
id3-001	0.3411	35	0.0043	45	0.0260	38	0.0043	54	0.0014	19
id3-002	0.3168	31	0.0030	40	0.0202	34	0.0032	47	0.0020	25
innovatrics-000	0.3392	33	0.0013	25	0.0087	23	0.0004	18	0.0027	31
innovatrics-001	0.3392	34	0.0013	26	0.0087	28	0.0004	19	0.0027	34
intellivision-001	0.5495	52	0.0052	48	0.0491	44	0.0042	53	0.0252	48
isityou-000	0.4714	44	0.0022	37	0.0665	47	0.0010	32	0.0116	42
itmo-002	0.5751	53	0.0068	51	0.0636	46	0.0029	46	0.0498	50
morpho-000	0.0000	8	0.0000	7	0.0000	13	0.0000	9	0.0000	9
morpho-002	0.0572	15	0.0009	18	0.0000	8	0.0004	16	0.0007	13
neurotechnology-001	0.2962	27	0.0000	8	0.0000	5	0.0000	3	0.0000	4
neurotechnology-002	0.2043	22	0.0000	9	0.0058	20	0.0000	6	0.0014	17
noblis-000	0.0000	5	0.0000	5	0.0000	7	0.0000	7	0.0000	6
ntechlab-002	0.0926	17	0.0009	16	0.0029	14	0.0005	20	0.0007	12
ntechlab-003	0.0926	18	0.0009	17	0.0029	17	0.0005	22	0.0007	16
pa-002	0.0000	1	0.0000	1	0.0000	1	0.0000	1	0.0000	1
rankone-002	0.0009	10	0.0001	11	0.0000	11	0.0000	11	0.0000	8
rankone-003	0.0009	9	0.0001	10	0.0000	9	0.0000	10	0.0000	7
samtech-000	0.5474	51	0.0052	49	0.0491	43	0.0042	52	0.0252	47
shaman-000	0.0000	4	0.0000	4	0.0000	6	0.0000	5	0.0000	5
shaman-001	0.0000	2	0.0000	2	0.0000	3	0.0000	2	0.0000	2
tevan-000	0.3373	32	0.0011	24	0.0000	12	0.0012	37	0.0020	29
tongyitrans-001	0.0000	7	0.0068	50	0.0462	41	0.0040	50	0.0055	38
tongyitrans-002	0.3609	38	0.0078	52	0.0462	42	0.0040	51	0.0055	39
toshiba-000	0.0000	6	0.0000	6	-	49	0.0000	8	-	49
toshiba-001	-	49	0.0000	3	-	49	0.0000	4	-	49
ultinous-000	-	49	0.0002	12	0.0000	4	0.0003	14	0.0000	3
vcog-002	0.2209	23	0.0021	35	0.0087	26	0.0019	42	0.0007	15
vigilantsolutions-002	0.3585	37	0.0010	21	0.0116	29	0.0004	17	0.0048	35
vigilantsolutions-003	-	49	0.0008	15	0.0058	22	0.0004	15	0.0014	20
visionlabs-001	0.2699	25	0.0014	27	0.0058	21	0.0014	39	0.0020	26
visionlabs-002	0.3063	28	0.0021	36	0.0087	24	0.0026	44	0.0007	14
vocord-002	0.3782	39	0.0015	29	0.0029	18	0.0037	48	0.0171	43
yisheng-000	0.4277	42	0.0016	32	0.0173	32	0.0006	25	0.0020	23
yisheng-001	0.4277	41	0.0016	31	0.0173	31	0.0006	24	0.0020	22
yitu-000	0.3475	36	0.0015	30	0.0029	16	0.0013	38	0.0014	18

Table 3: FTE is the proportion of failed template generation attempts. Failures can occur because the software throws an exception, or because the software electively refuses to process the input image. This would typically occur if a face is not detected. FTE is measured as the number of function calls that give a non-zero error code, OR that give a “small” template. This is defined as one whose size is less than 0.3 times the median template size. This second rule is needed because some algorithms incorrectly fail to return a non-zero error code when template generation fails.

¹ The effects of FTE are included in the accuracy results of this report by regarding any template comparison involving a failed template enrollment to produce a low similarity score. Thus higher FTE results in higher FNMR.

5.4 Recognition accuracy

Core algorithm accuracy is stated via:

▷ **Cooperative subjects**

- The summary table of Figure 2;
- The visa image DETs of Figures 4 and 5;
- The mugshot DETs of Figure 6 ;
- The selfie-portrait DETs of Figure 7;
- The webcam-portrait DETs of Figure 8;

▷ **Non-cooperative subjects**

- The photojournalism DET of Figure 9
- The sensitivity of photojournalism FNMR to relative yaw angles in Figure 10.
- The sensitivity of photojournalism FMR to relative yaw angles in Figure 11.
- The child-exploitation DET of Figure 12;
- The child-exploitation CMC of Figure 13.

Figure 18 shows dependence of false match rate on algorithm score threshold. This allows a deployer to set a threshold to target a particular false match rate appropriate to the security objectives of the application.

Figure 20 likewise shows FMR(T) but for mugshots, and specially four subsets of the population.

Note that in both the mugshot and visa sets false match rates vary with the ethnicity, age, and sex, of the enrollee and impostor - see section 5.6.

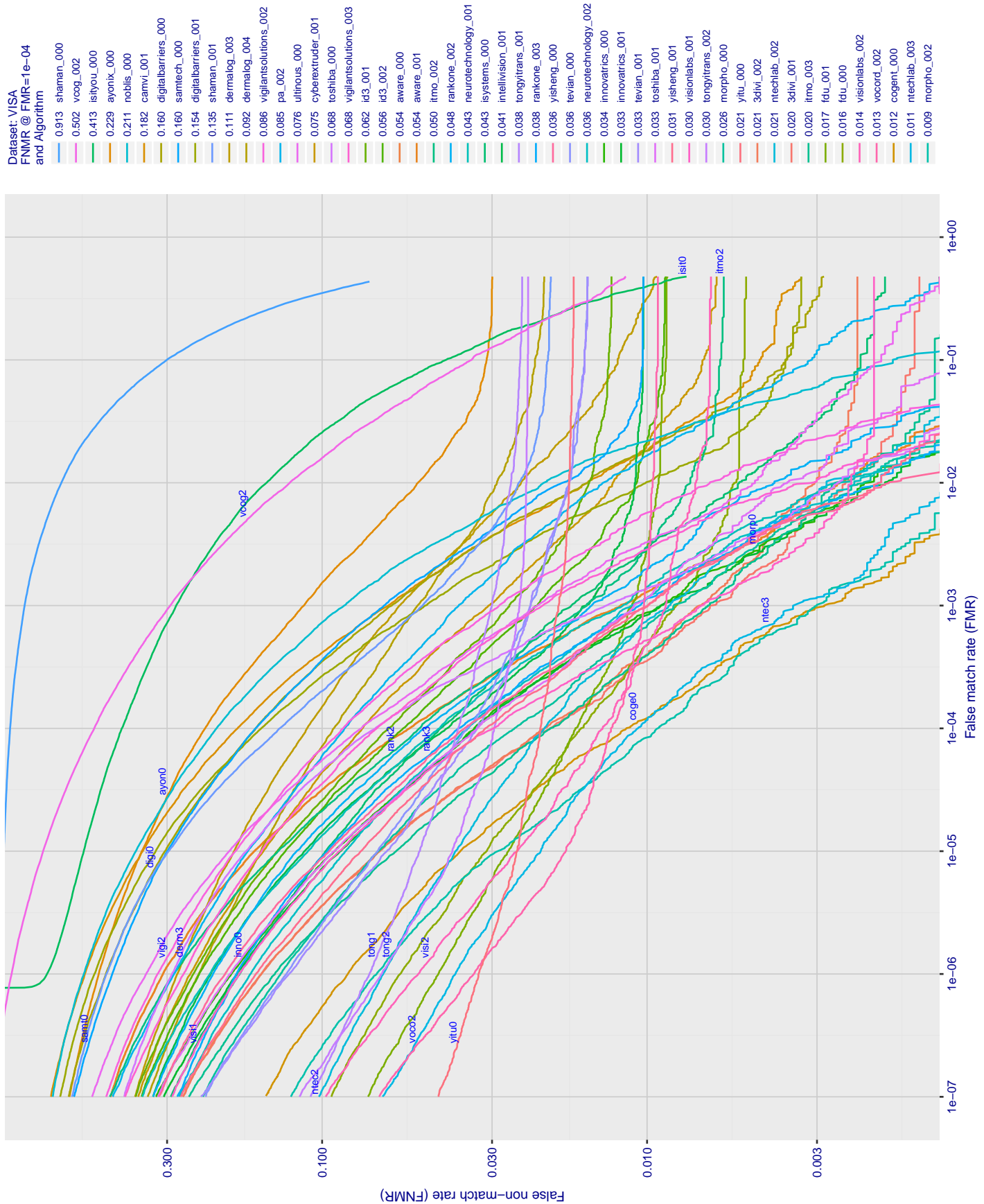


Figure 4: For the visa images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T . The scales are logarithmic in order to show many decades of FMR.

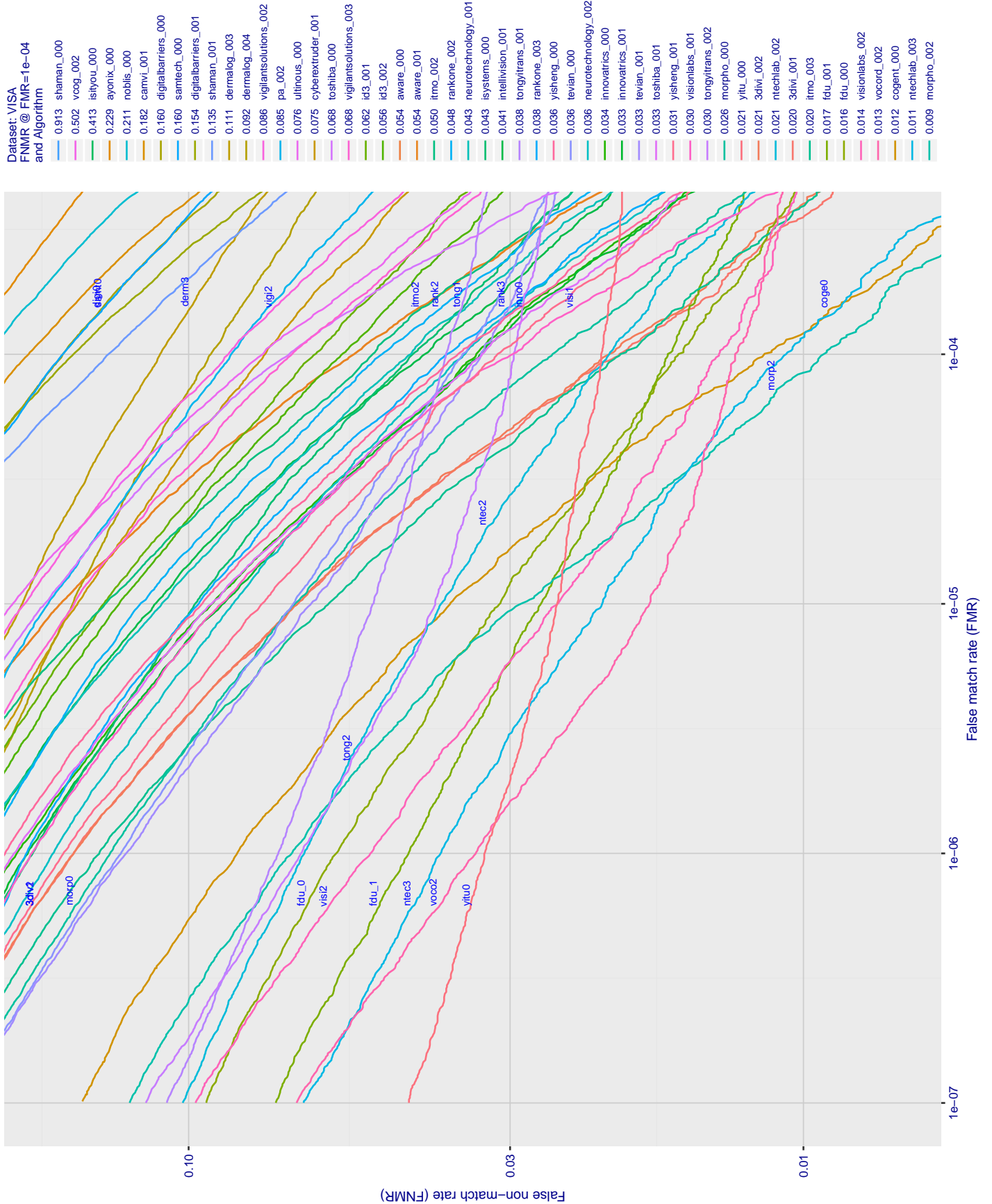


Figure 5: For the visa images, but now just for low FMR, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T . The scales are logarithmic in order to show many decades of FMR.

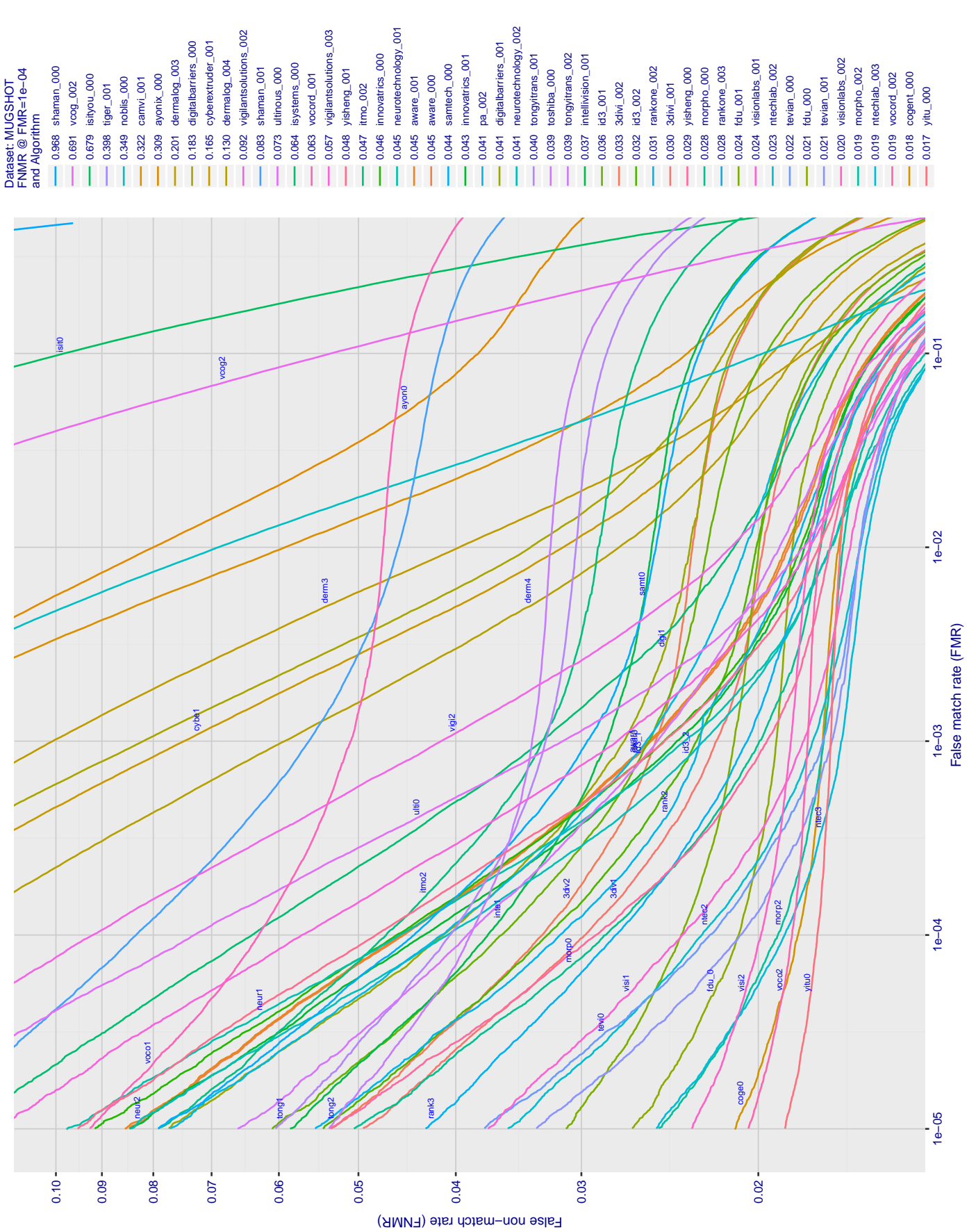


Figure 6: For the mugshot images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T . The scales are logarithmic in order to show decades of FMR.



Figure 7: For the selfie-to-portrait comparisons, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T . The scales are logarithmic in order to show several decades of FMR. **Caution: The FNMR values here are optimistic statements of accuracy because the image pairs were collected on the same day. This is known across biometrics to give better accuracy, and is operationally relevant only in special cases.**

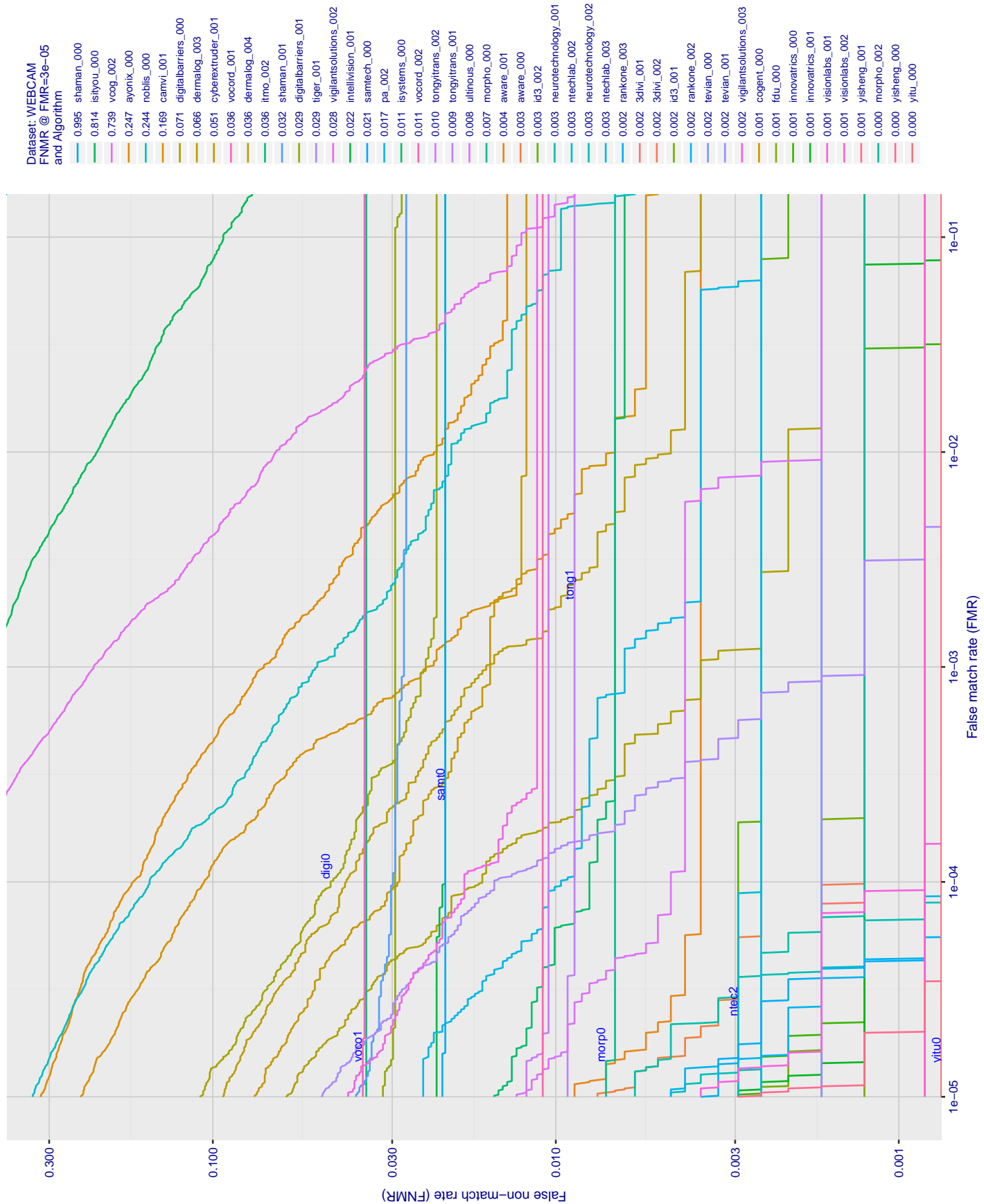


Figure 8: For the webcam-to-portrait comparisons, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T . The scales are logarithmic in order to show several decades of FMR. **Caution:** The FNMR values **here** are **optimistic statements of accuracy because the image pairs were collected on the same day**. This is known across biometrics to give better accuracy, and is operationally relevant only in special cases.

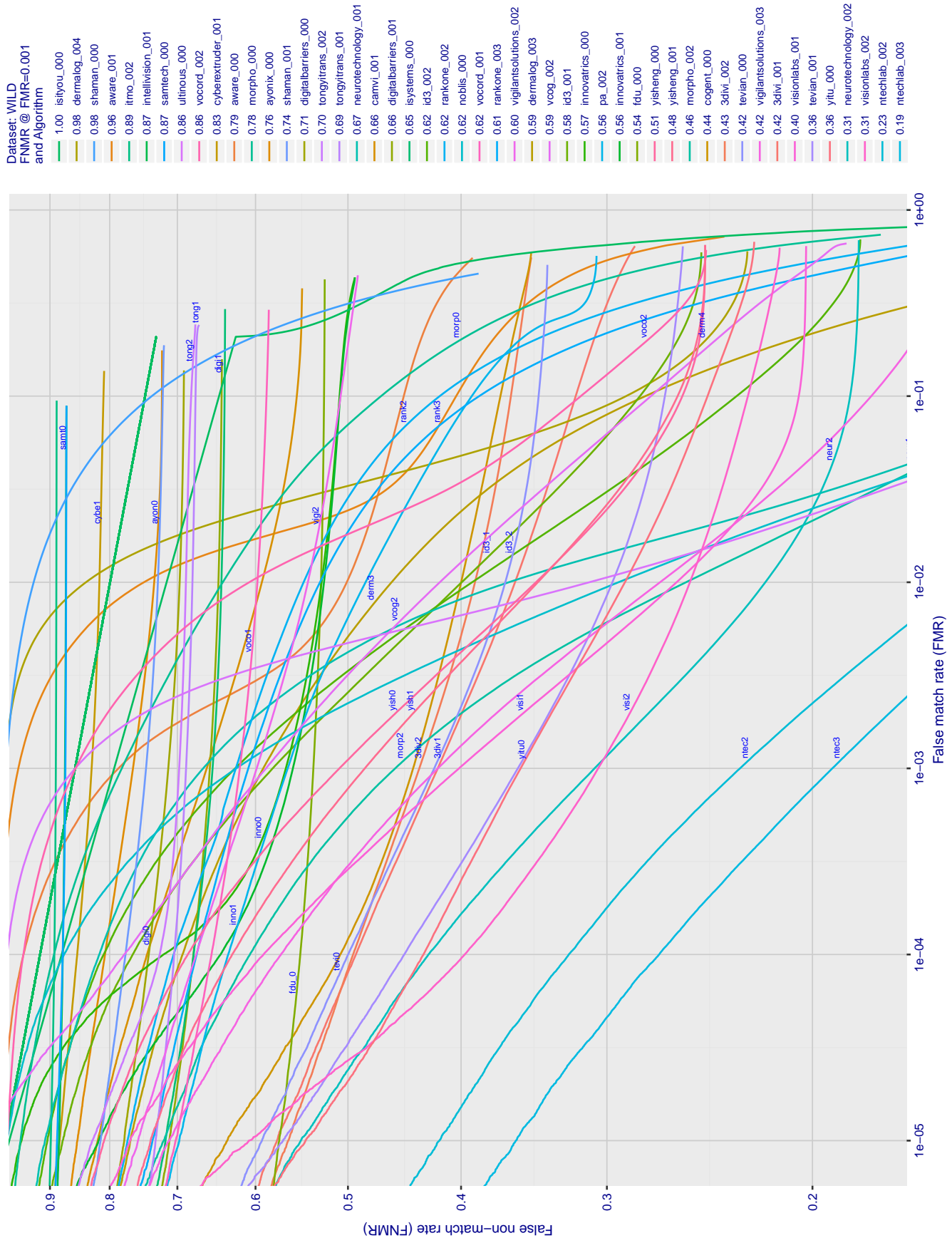


Figure 9: For the wild image comparisons, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T . The scales are logarithmic in order to show several decades of FMR.

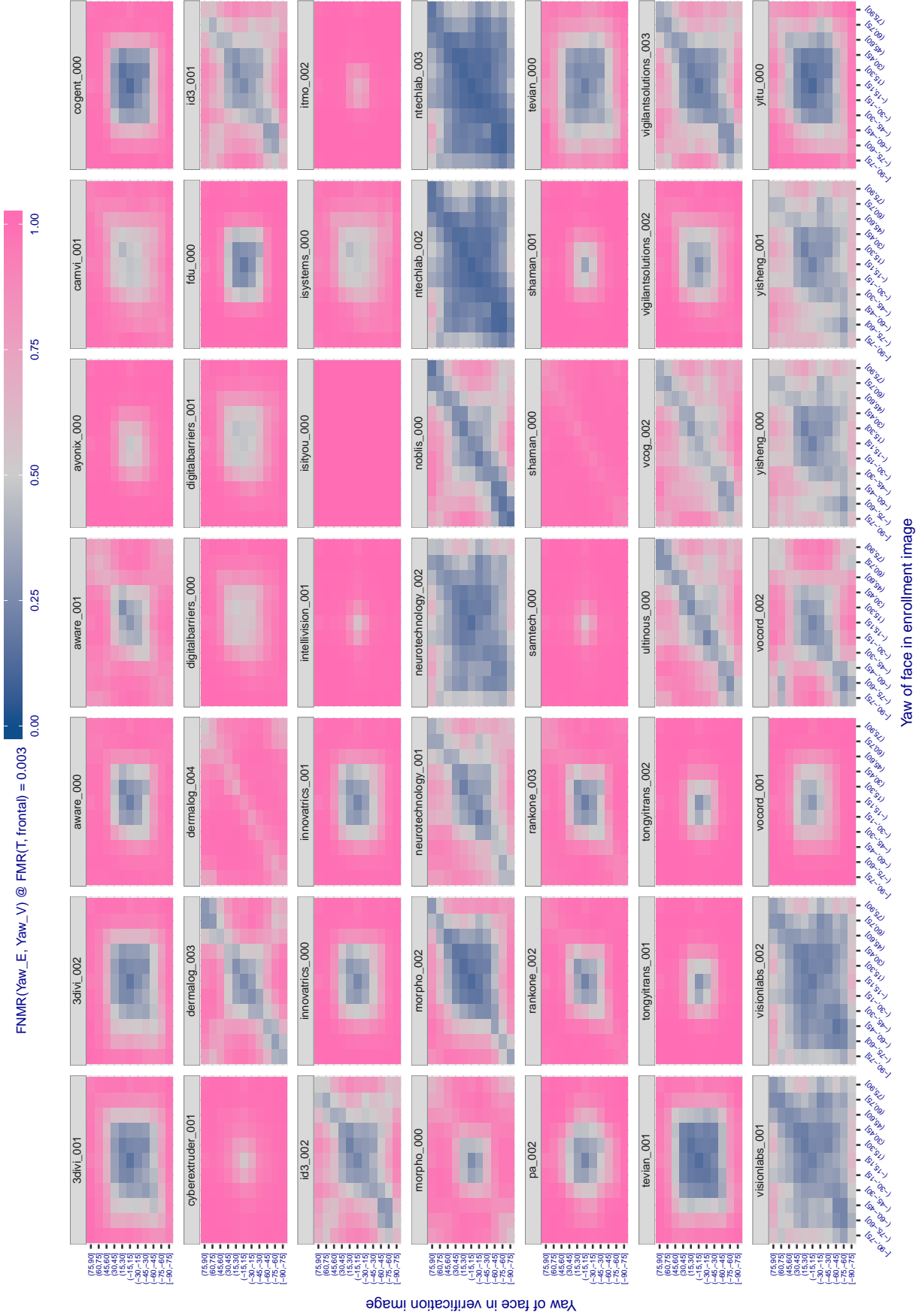
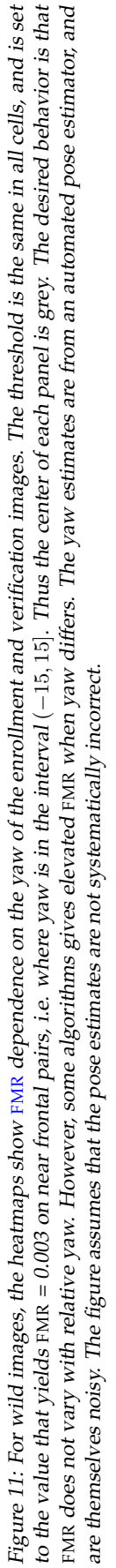


Figure 10: For wild images, the heatmap show FNMR as a function of the yaw of the enrollment and verification images. The threshold is the same in all cells, and is set to the value that yields FMR = 0.003 on near frontal pairs i.e. where yaw is in the interval $(-15, 15]$. Poor algorithms give generally red figures. The better algorithms show a) diagonal dominance, indicating ability to authenticate when pairs have the same yaw angle, and b) off-diagonal cross-pose capability also. The yaw estimates are from an automated pose estimator, and are themselves noisy. The figure assumes that the pose estimates are not systematically incorrect.



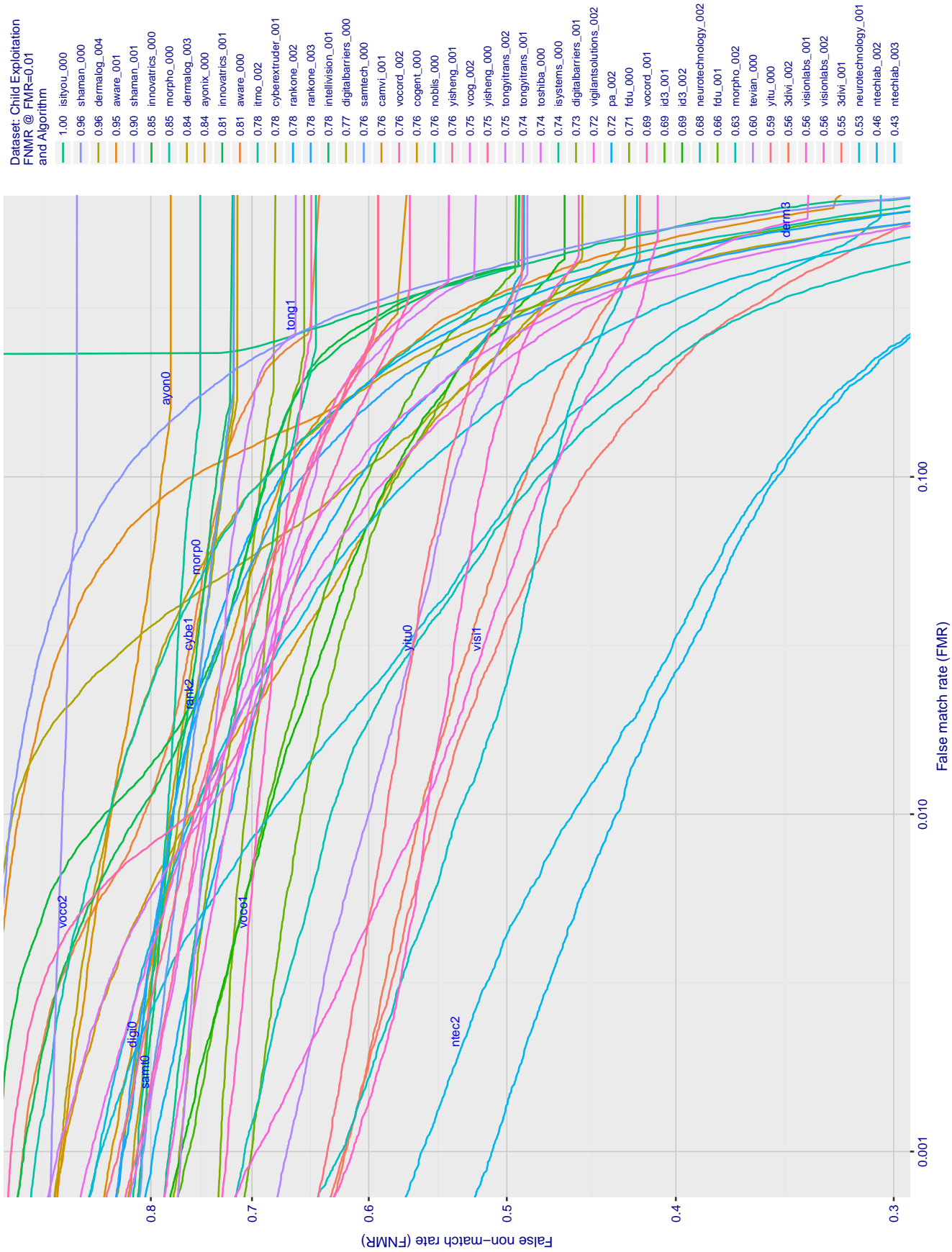


Figure 12: For child exploitation images, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T . The scales are logarithmic in order to show many decades of FMR. Accuracy is poor because many images have adverse quality characteristics, and because detection and enrollment fails.

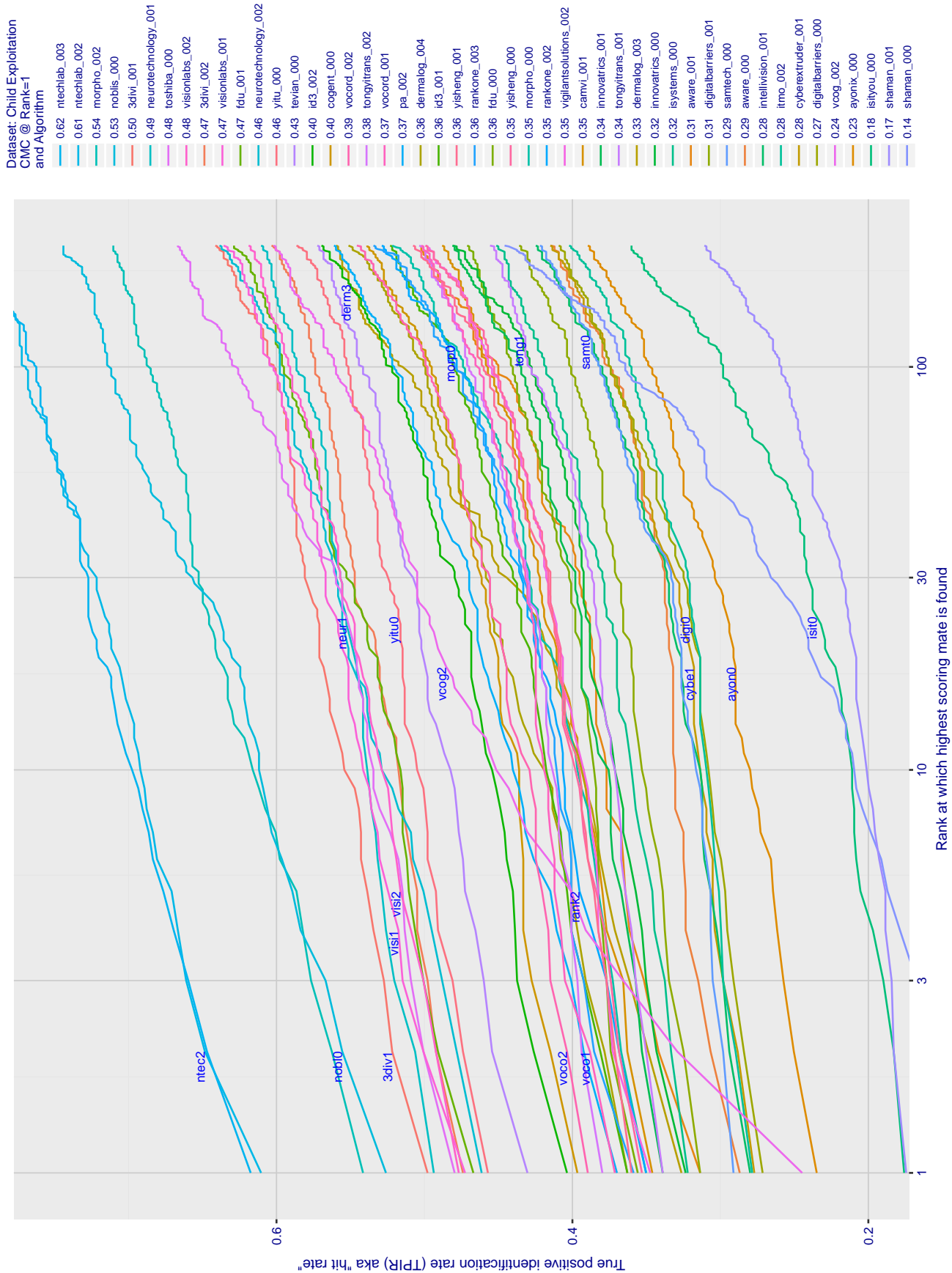
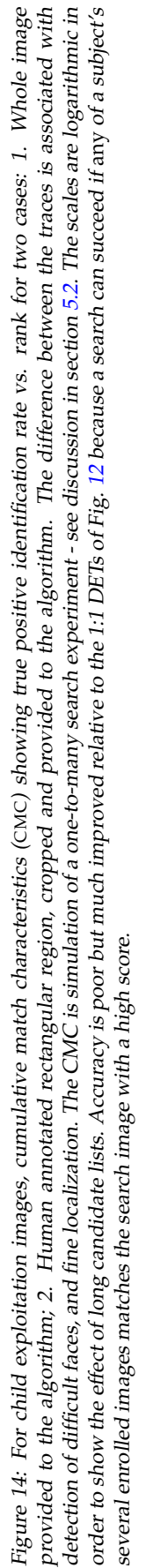


Figure 13: For child exploitation images, cumulative match characteristics (CMC) showing true positive identification rate vs. rank. This is simulation of a one-to-many search experiment - see discussion in section 5.2. The scales are logarithmic in order to show the effect of long candidate lists. Accuracy is poor but much improved relative to the 1:1 DETs of Fig. 12 because a search of a subject's several enrolled images matches the search image with a high score.



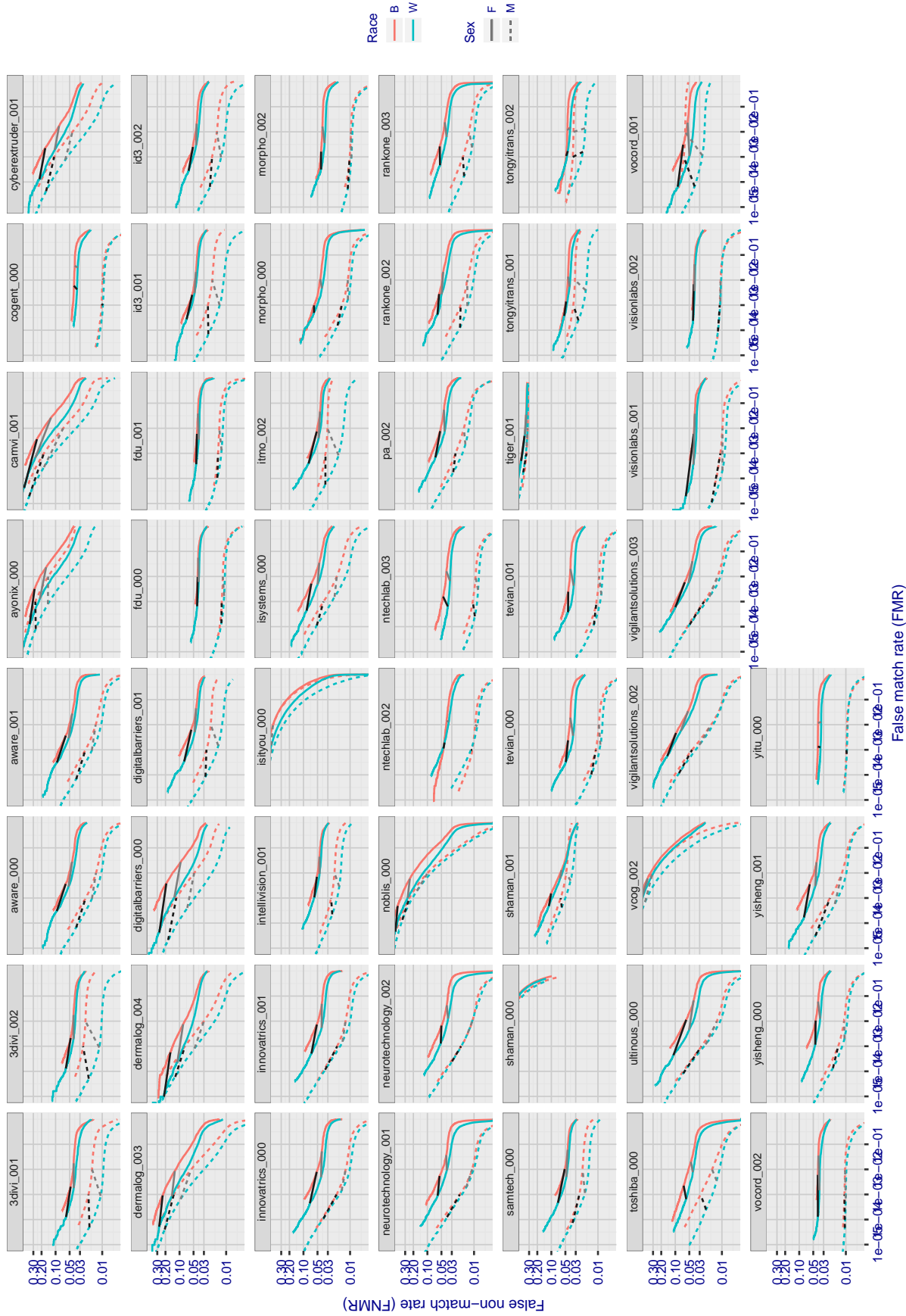


Figure 15: For the mugshot images, error tradeoff characteristics for white females, black females, black males and white males. The grey lines correspond to fixed thresholds, showing how both FNMR and FMR vary at one operating threshold. Important: Many of the plots will naively be read as saying whites gives lower error rates than blacks because the blue traces lie beneath the red ones. However, this is misleading and incomplete: The grey lines show the traces are generally shifted horizontally. Thus for the dermalog-001 algorithm FNMR for whites is higher than for blacks at a fixed threshold but, at the same time, FMR is higher for blacks - see Figure 20. As access control systems almost always operate at a fixed threshold, the naive interpretation is incorrect.

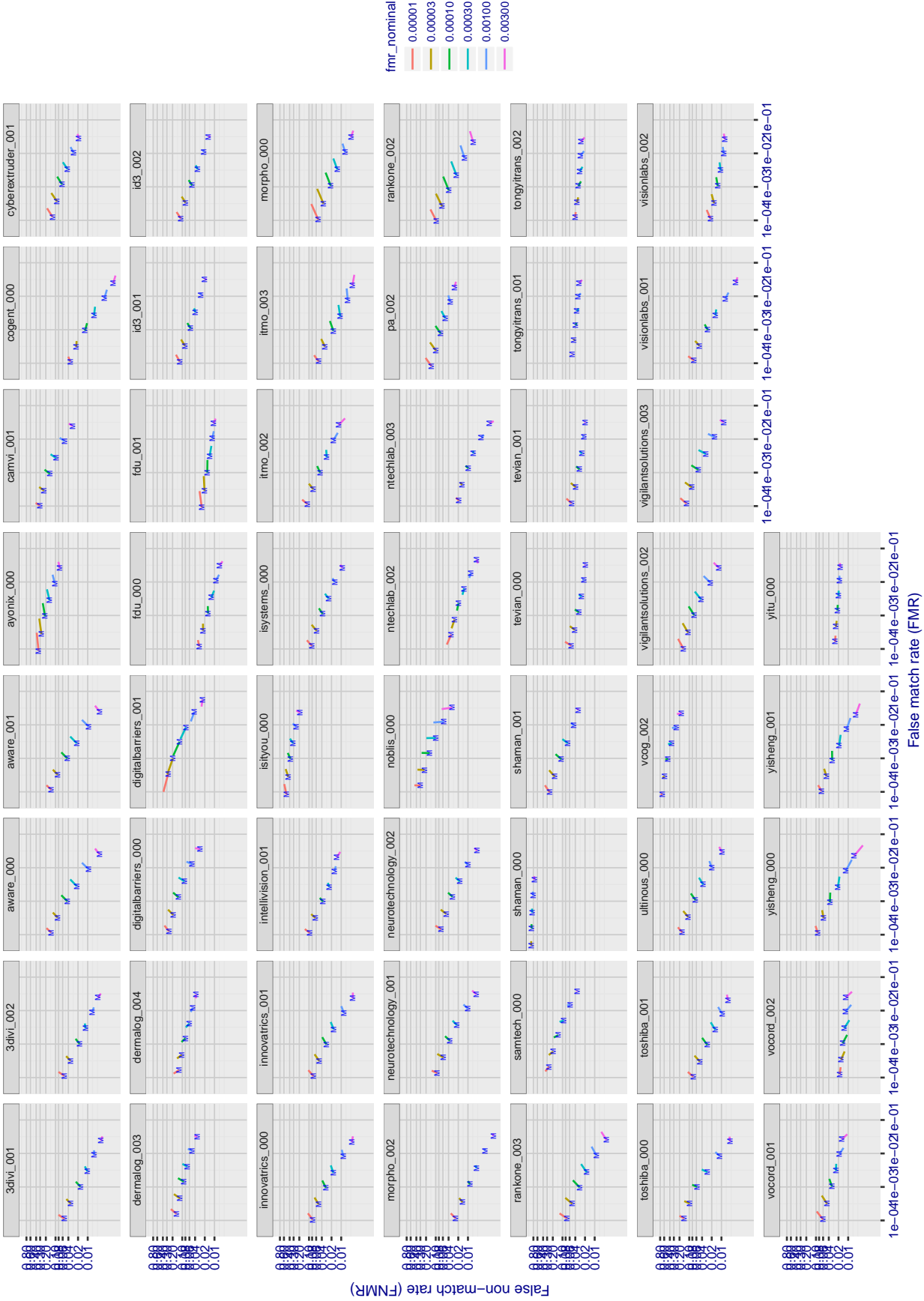


Figure 16: For the visa images, FNMR and FMR at six operating points along the DET characteristic. At each point a line is drawn between $(FMR, FNMR)_{\text{MALE}}$ and $(FMR, FNMR)_{\text{FEMALE}}$ showing how which sex has lower FMR and/or FNMR. The "M" label denotes male, the other end of the line corresponds to female. The six operating thresholds are selected to give the nominal false match rates given in the legend, and are computed over all impostor pairs regardless of age, sex, and place of birth. The plotted FMR values are broadly an order of magnitude larger than the nominal rates because FMR is computed over demographically-matched impostor pairs i.e individuals of the same sex, from the same geographic region (see section 5.6.1), and the same age group (see section 5.6.2).

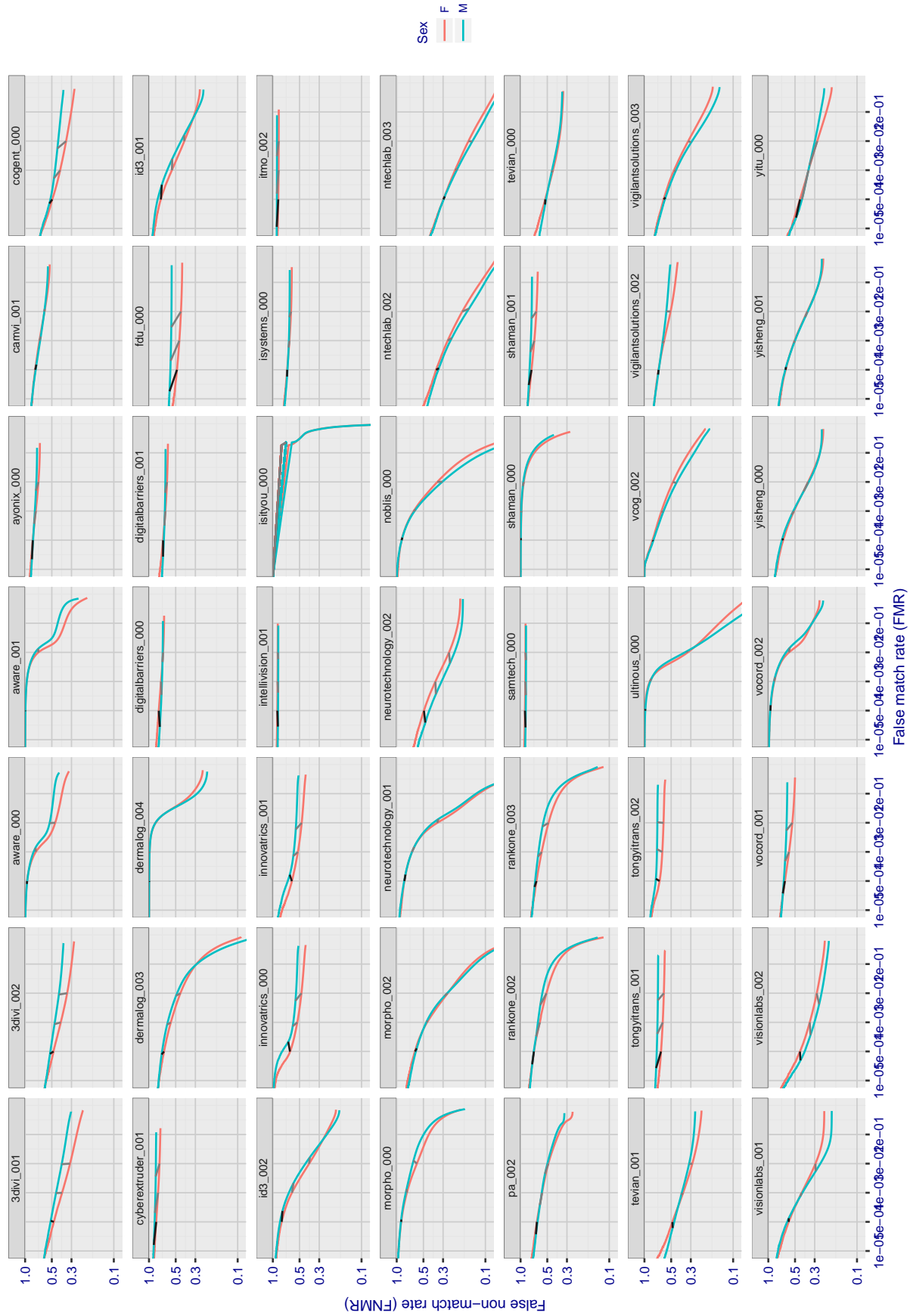
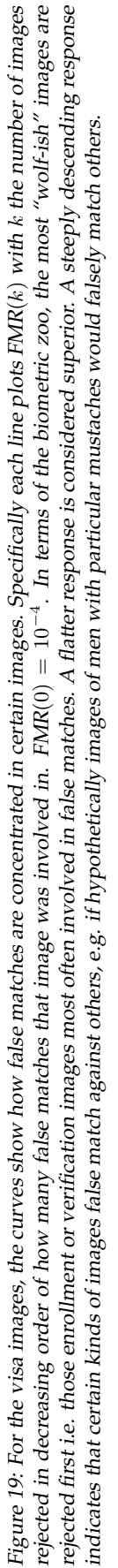


Figure 17: For the wild image comparisons, detection error tradeoff (DET) characteristics showing false non-match rate vs. false match rate plotted parametrically on threshold, T. Error rates are higher here than in the generic wild DET (Fig 9) because the impostor pairs here are same-sex only. The scales are logarithmic in order to show several decades of FMR.





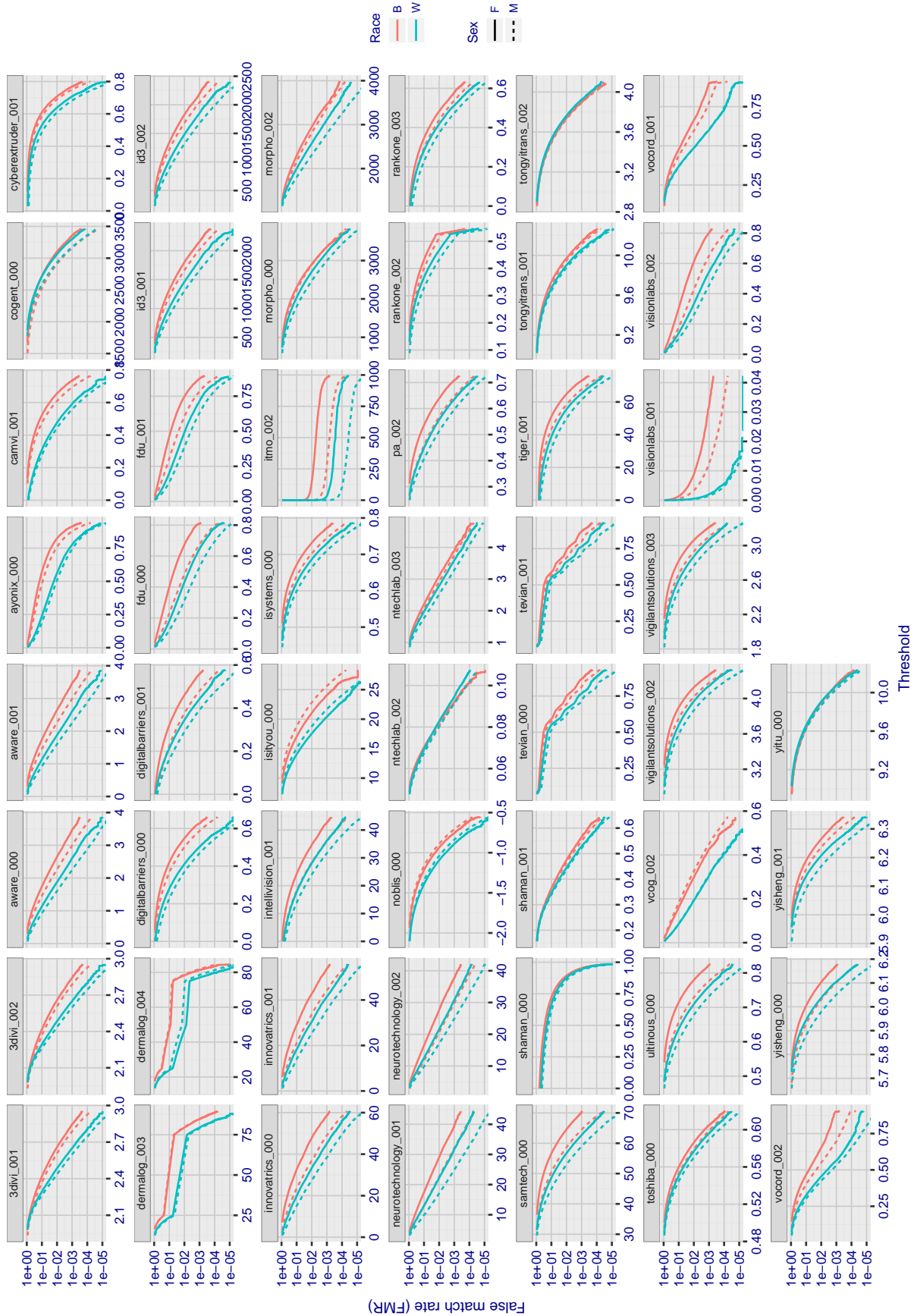


Figure 20: For the mugshot images, the false match calibration curves show false match rate vs. threshold. Separate curves appear for white females, black females, black males and white males.

5.5 Genuine distribution stability

5.5.1 Effect of birth place on the genuine distribution

Background: Both skin tone and bone structure vary geographically. Prior studies have reported variations in FNMR and FMR.

Goal: To measure false non-match rate (FNMR) variation with country of birth.

Methods: Thresholds are determined that give $FMR = \{0.001, 0.0001\}$ over the entire impostor set. Then FNMR is measured over 1000 bootstrap replications of the genuine scores. Only those countries with at least 140 individuals are included in the analysis.

Results: Figure 21 shows FNMR by country of birth for the two thresholds.

Caveats: The results may not relate to subject-specific properties. Instead they could reflect image-specific quality differences, which could occur due to collection protocol or software processing variations.



Figure 21: For the visa images, the dots show FNMR by country of birth for two operating thresholds corresponding to $FMR = \{0.001, 0.0001\}$ computed over all $O(10^{10})$ impostor scores. The figures shows an order of magnitude variation in FNMR across country of birth; these effects are due to quality variations. The least accurate countries vary by algorithm.

5.5.2 Effect of age on genuine subjects

Background: Faces change appearance throughout life. Face recognition algorithms have previously been reported to give better accuracy on older individuals (See NIST IR 8009).

Goal: To quantify false non-match rates (FNMR) as a function of age. We do not aim to quantify ageing effects here as the separation between two samples is limited to just a few years.

Methods: Using the visa images, thresholds are determined that give $FMR = 0.001$ and 0.0001 over the entire impostor set. Then FNMR is measured over 1000 bootstrap replications of the genuine scores.

Results: For the visa images, Figure 22 shows how false non-match rates for genuine users, as a function of age group.

The notable aspects are:

- ▷ Younger subjects give considerably higher FNMR. This is likely due to rapid growth and change in facial appearance.
- ▷ FNMR trends down throughout life. The last bin, $AGE > 72$, contains fewer than 140 mated pairs, and may be affected by small sample size.

Caveats: None.

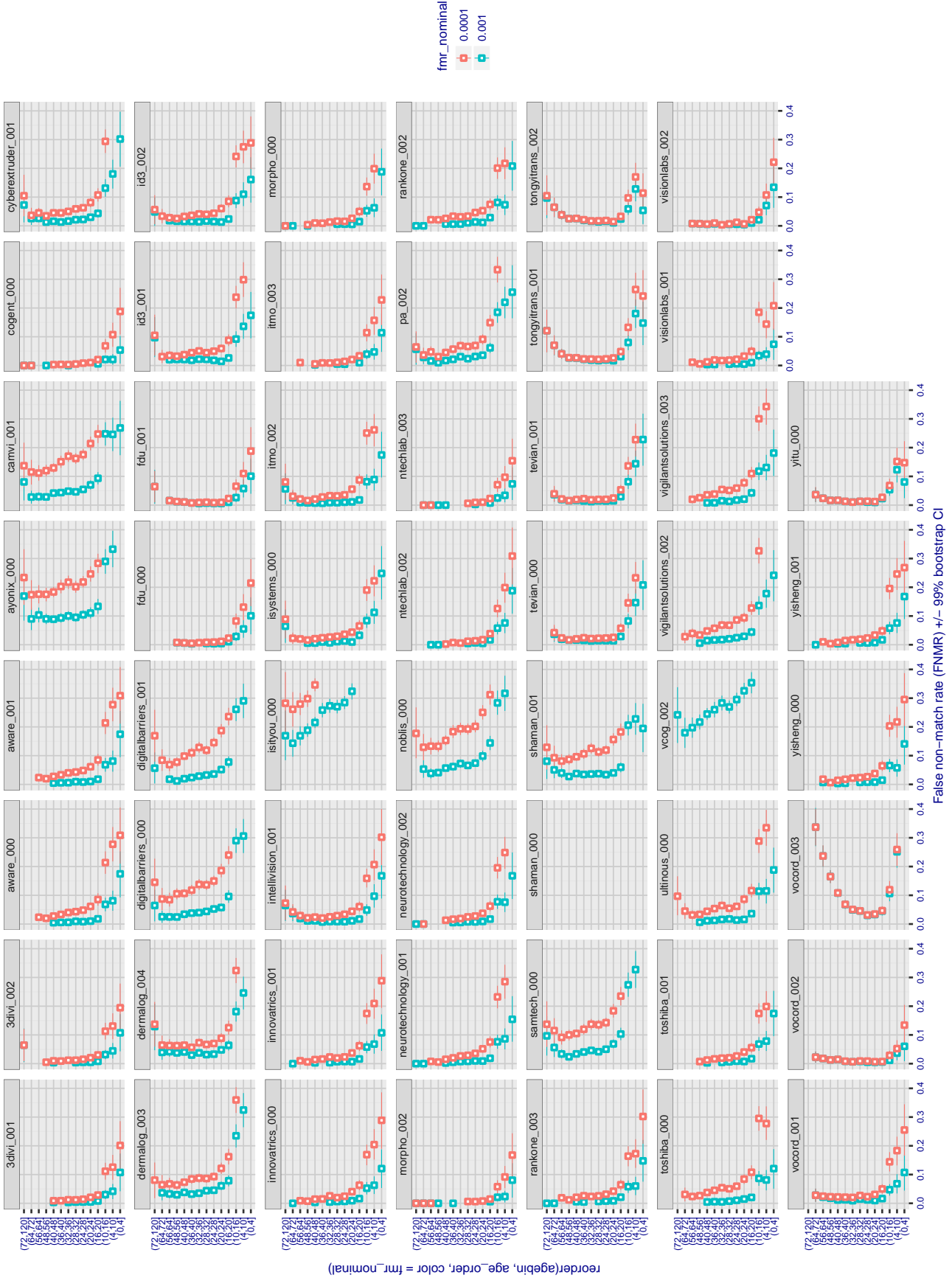


Figure 22: For the visa images, the dots show FNMR by age group for two operating thresholds corresponding to $FMR = \{0.001, 0.0001\}$ computed over all $O(10^{10})$ impostor scores. Given a pair of face images taken at different times, we assign a false non-match to the bin that is the arithmetic average of the subject's ages. This plot shows only the effect of age, not ageing. The number of comparisons in each bin is generally in the thousands. However the FNMR for the first and last bins are each computed over fewer than 150 comparisons.

5.6 Impostor distribution stability

5.6.1 Effect of birth place on the impostor distribution

Background: Facial appearance varies geographically, both in terms of skin tone, cranio-facial structure and size. This section addresses whether false match rates vary intra- and inter-regionally.

Goals:

- ▷ To show the effect of birth region of the impostor and enrollee on false match rates.
- ▷ To determine whether some algorithms give better impostor distribution stability.

Methods:

- ▷ For the visa images, NIST defined 10 regions: Sub-Saharan Africa, South Asia, Polynesia, North Africa, Middle East, Europe, East Asia, Central and South America, Central Asia, and the Caribbean.
- ▷ For the visa images, NIST mapped each country of birth to a region. There is some arbitrariness to this. For example, Egypt could reasonably be assigned to the Middle East instead of North Africa. An alternative methodology could, for example, assign the Philippines to *both* Polynesia and East Asia.
- ▷ FMR is computed for cases where all face images of impostors born in region r_2 are compared with enrolled face images of persons born in region r_1 .

$$\text{FMR}(r_1, r_2, T) = \frac{\sum_{i=1}^{N_{r_1, r_2}} H(s_i - T)}{N_{r_1, r_2}} \quad (5)$$

where the same threshold, T , is used in all cells, and H is the unit step function. The threshold is set to give $\text{FMR}(T) = 0.001$ over the entire set of visa image impostor comparisons.

- ▷ This analysis is then repeated by country-pair, but only for those country pairs where both have at least 1000 images available. The countries¹ appear in the axes of graphs that follow.
- ▷ The mean number of impostor scores in any cross-region bin is 33 million. The smallest number of impostor scores in any bin is 135000, for Central Asia - North Africa. While these counts are large enough to support reasonable significance, the number of individual faces is much smaller, $O(N^{0.5})$.
- ▷ The numbers of impostor scores in any cross-country bin is shown in Figure 123.

Results: Subsequent figures show heatmaps that use color to represent the base-10 logarithm of the false match rate. Red colors indicate high (bad) false match rates. Dark colors indicate benign false match rates. There are two series of graphs corresponding to aggregated geographical regions, and to countries. The notable observations are:

- ▷ The on-diagonal elements correspond to within-region impostors. FMR is generally above the nominal value of $\text{FMR} = 0.001$. Particularly there is usually higher FMR in, Sub-Saharan Africa, South Asia, and the Caribbean. Europe and Central Asia, on the other hand, usually give FMR closer to the nominal value.
- ▷ The off-diagonal elements correspond to across-region impostors. The highest FMR is produced between the Caribbean and Sub-Saharan Africa.
- ▷ Algorithms vary.

¹These are Argentina, Australia, Brazil, Chile, China, Costa Rica, Cuba, Czech Republic, Dominican Republic, Ecuador, Egypt, El Salvador, Germany, Ghana, Great Britain, Greece, Guatemala, Haiti, Hong Kong, Honduras, Indonesia, India, Israel, Jamaica, Japan, Kenya, Korea, Lebanon, Mexico, Malaysia, Nepal, Nigeria, Peru, Philippines, Pakistan, Poland, Romania, Russia, South Africa, Saudi Arabia, Thailand, Trinidad, Turkey, Taiwan, Ukraine, Venezuela, and Vietnam.

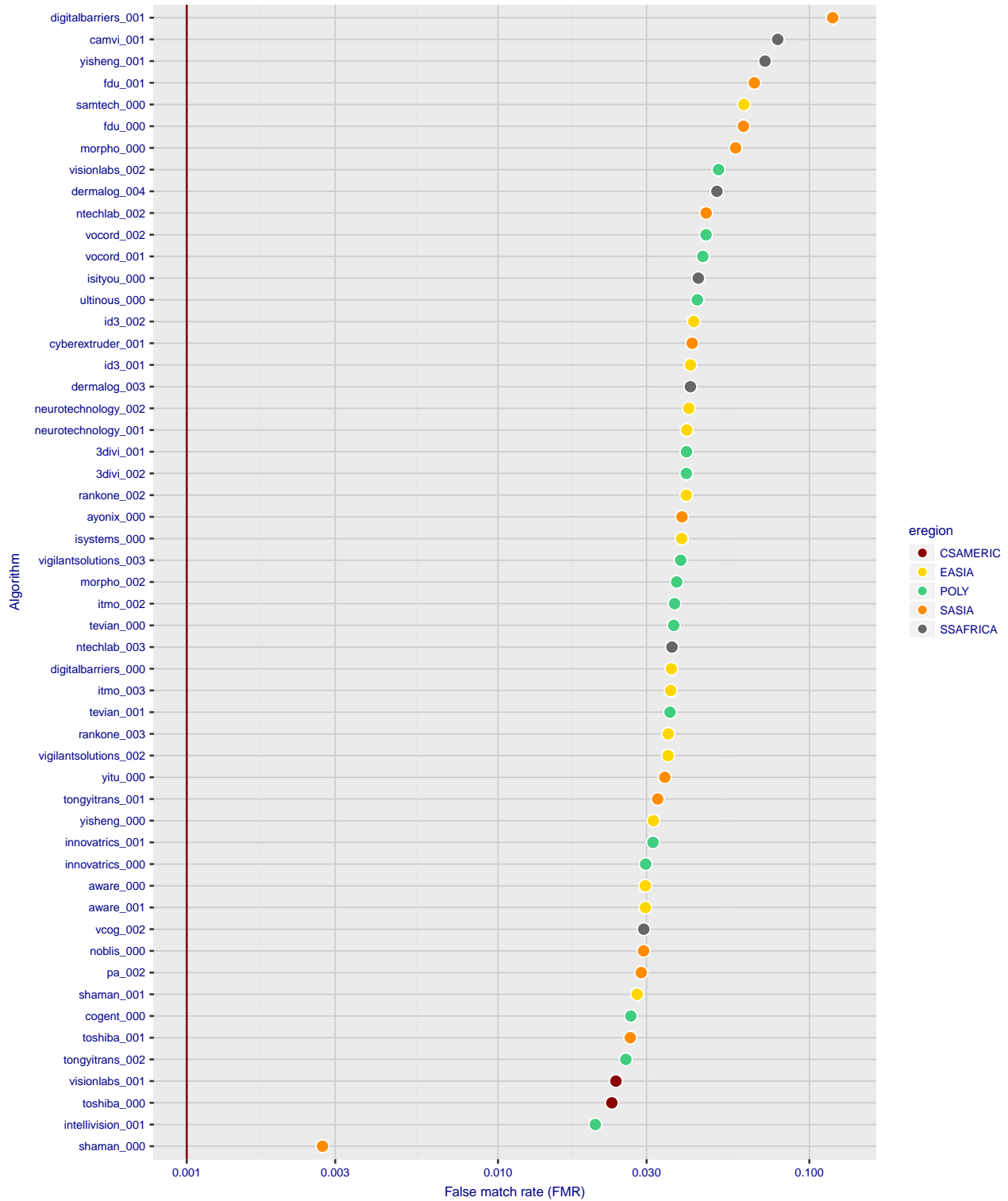


Figure 23: For the visa images, the dots show FMR for impostor comparisons of individuals of the same sex and same age group for the region of the world that gives the worst (highest) FMR when the threshold is set to give FMR = 0.001 (red vertical line) over all $O(10^{10})$ impostor scores i.e. zero-effort. The shift of the dots to right shows massive increases in FMR when impostors have the same sex, age, and region of birth. The color code indicates which region gives the worst case FMR. If the observed variation is due to the prevalence of one kind of images in the training imagery, then algorithms developed on one kind of data might be expected to give higher FMR on other kinds.

- ▷ We computed the same quantities for a global FMR = 0.0001. The effects are similar.

Caveats:

- ▷ The effects of variable impostor rates on one-to-many identification systems may well differ from what's implied by these one-to-one verification results. Two reasons for this are a) the enrollment galleries are usually imbalanced across countries of birth, age and sex; b) one-to-many identification algorithms often implement techniques aimed at stabilizing the impostor distribution. Further research is necessary.
- ▷ In principle, the effects seen in this subsection could be due to differences in the image capture process. We consider this unlikely since the effects are maintained across geography - e.g. Caribbean vs. Africa, or Japan vs. China.

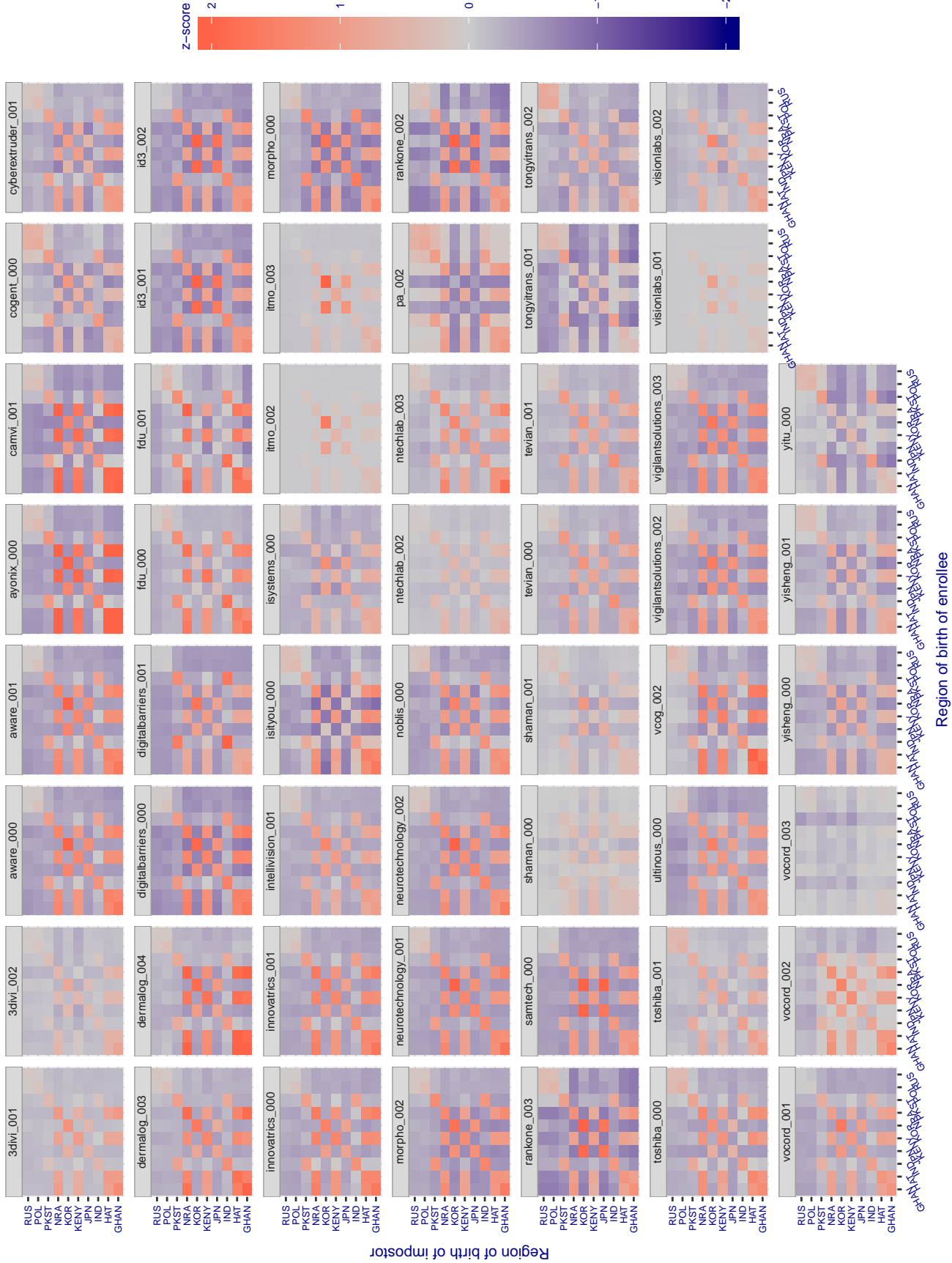


Figure 24: For visa images, the heatmap shows how the mean of the impostor distribution for the country pair (a,b) is shifted relative to the mean of the global impostor distribution, expressed as a number of standard deviations of the global impostor distribution. This statistic is designed to show shifts in the entire impostor distribution, not just tail effects that manifest as the anomalously high (or low) false match rates that appear in the subsequent figures. The countries are chosen to show that skin tone alone does not explain impostor distribution shifts. The reduced shift in Asian populations with the Yitu and TongYiTrans algorithms, is accompanied by positive shifts in the European populations. This reversal relative to most other algorithms, may derive from use of nationally weighted training sets. The Visionlabs algorithm appears most insensitive to country effects. The figure is computed from same-sex and same-age impostor pairs.

Cross region FMR at threshold $T = 2.899$ for algorithm 3divi_001, giving $FMR(T) = 0.0001$ globally.

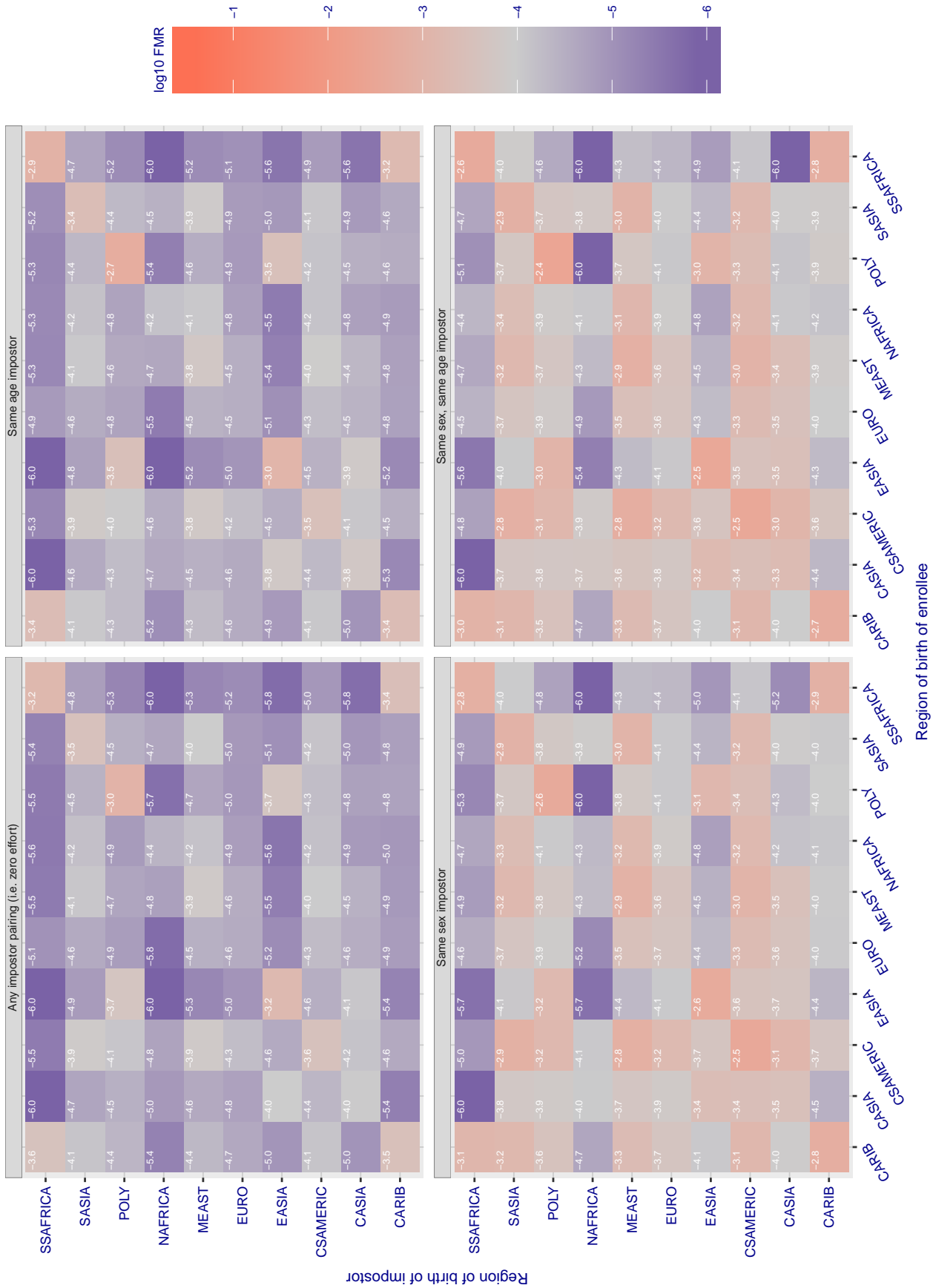


Figure 25: For algorithm 3divi-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 2.899$ for algorithm 3divi_002, giving $FMR(T) = 0.0001$ globally.

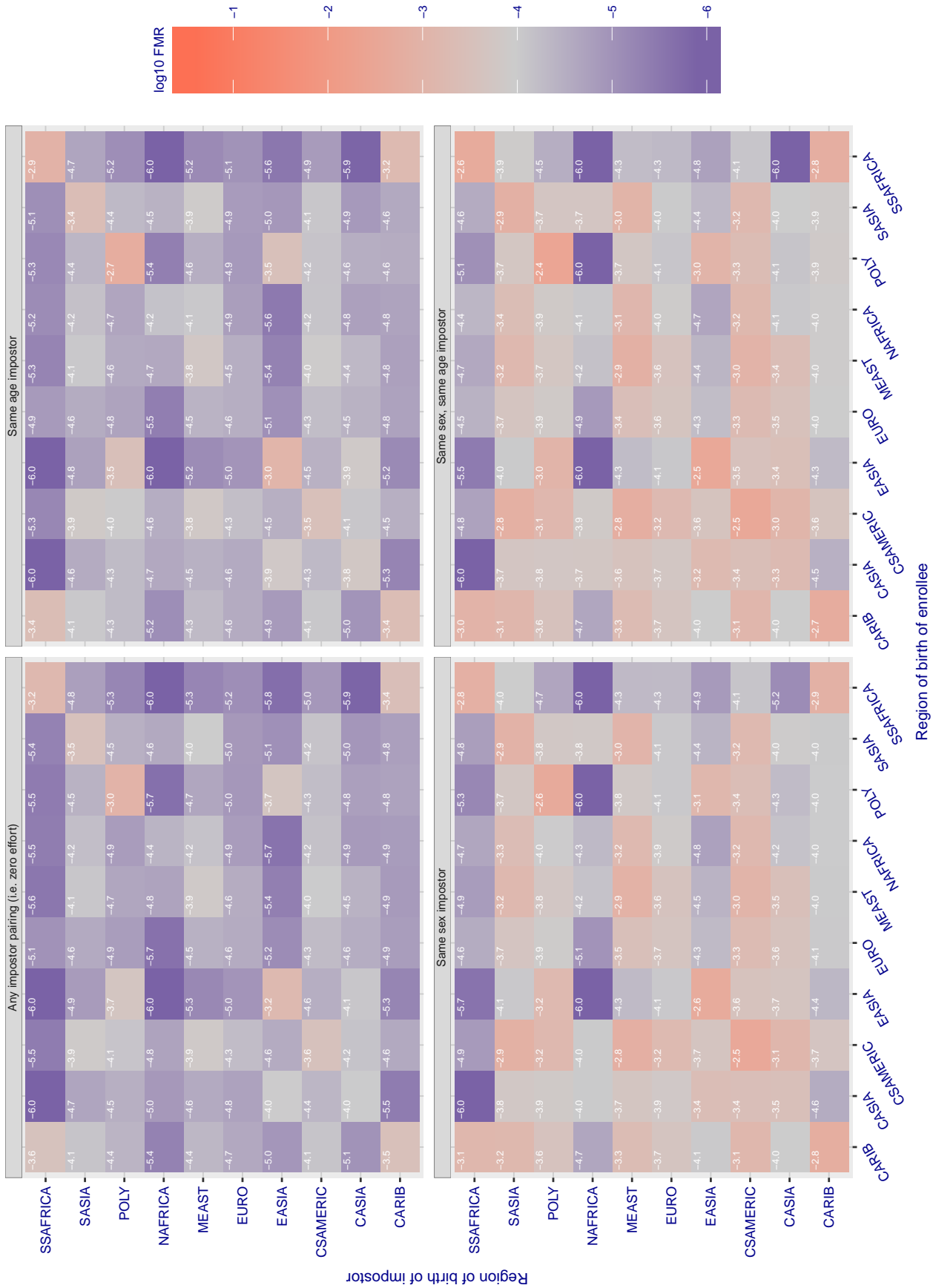


Figure 26: For algorithm 3divi-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 4.029$ for algorithm aware_000, giving $FMR(T) = 0.0001$ globally.

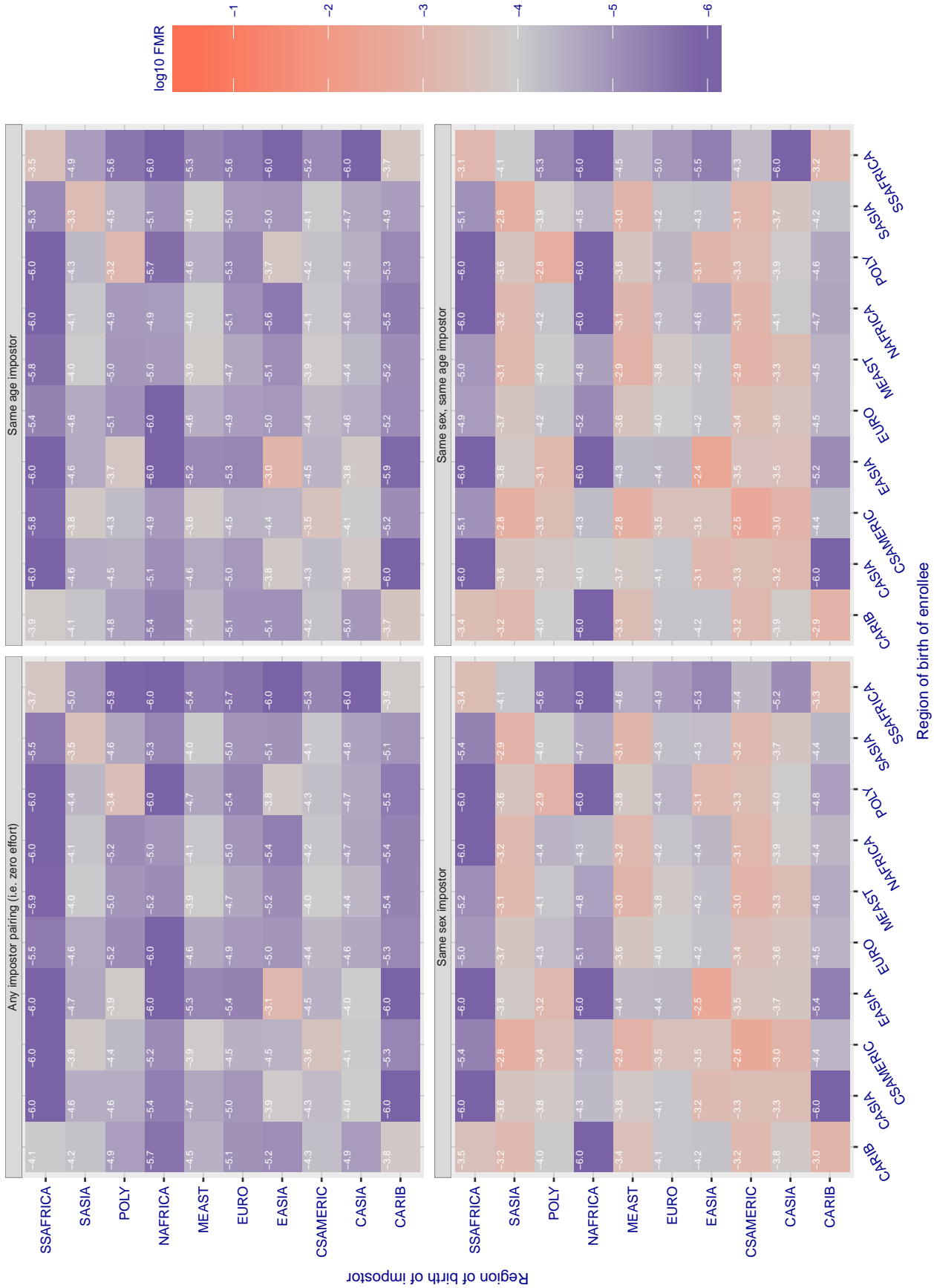


Figure 27: For algorithm aware-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 4.029$ for algorithm aware_001, giving $FMR(T) = 0.0001$ globally.

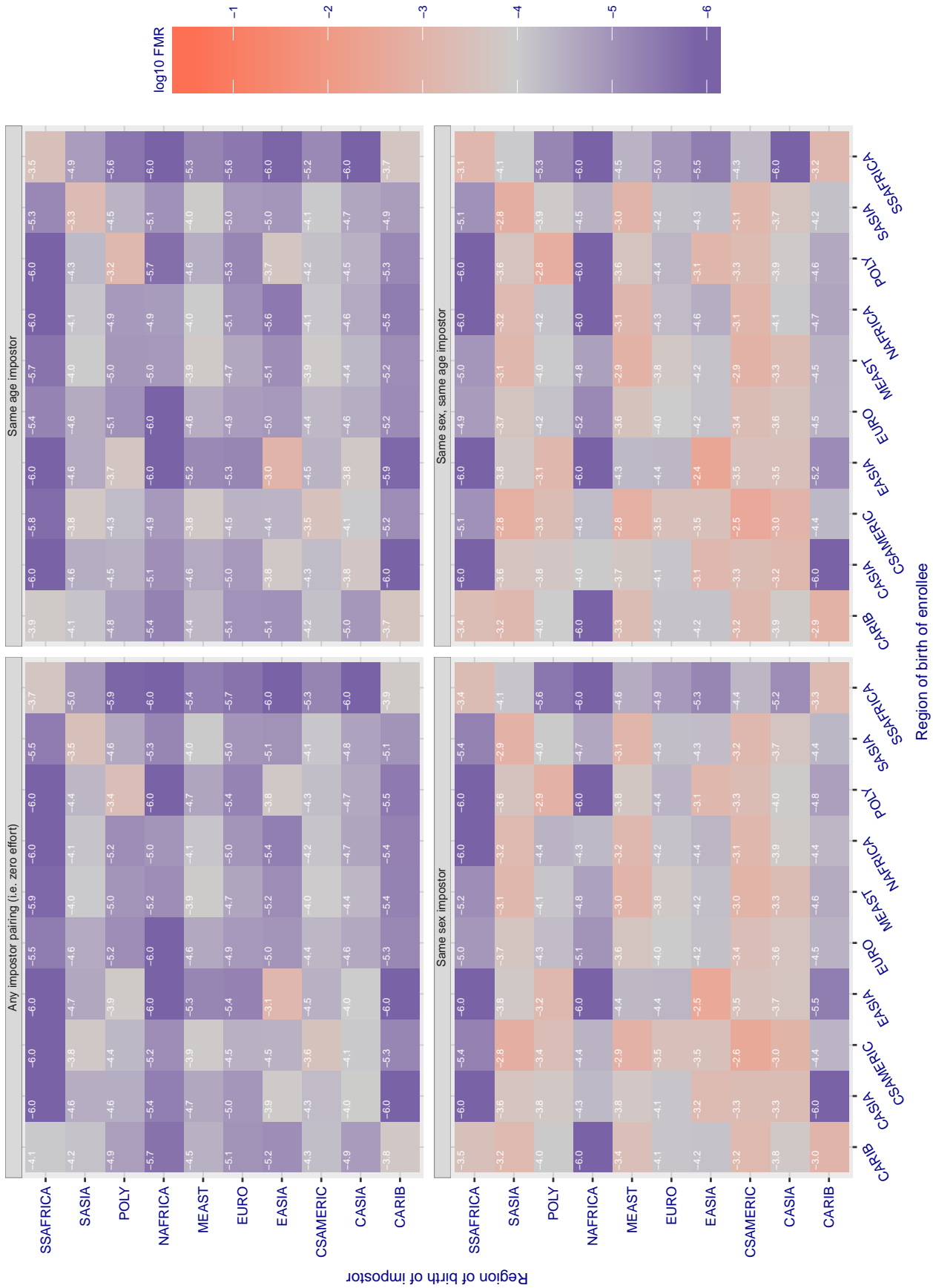


Figure 28: For algorithm aware-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.919$ for algorithm ayonix_000, giving $FMR(T) = 0.0001$ globally.

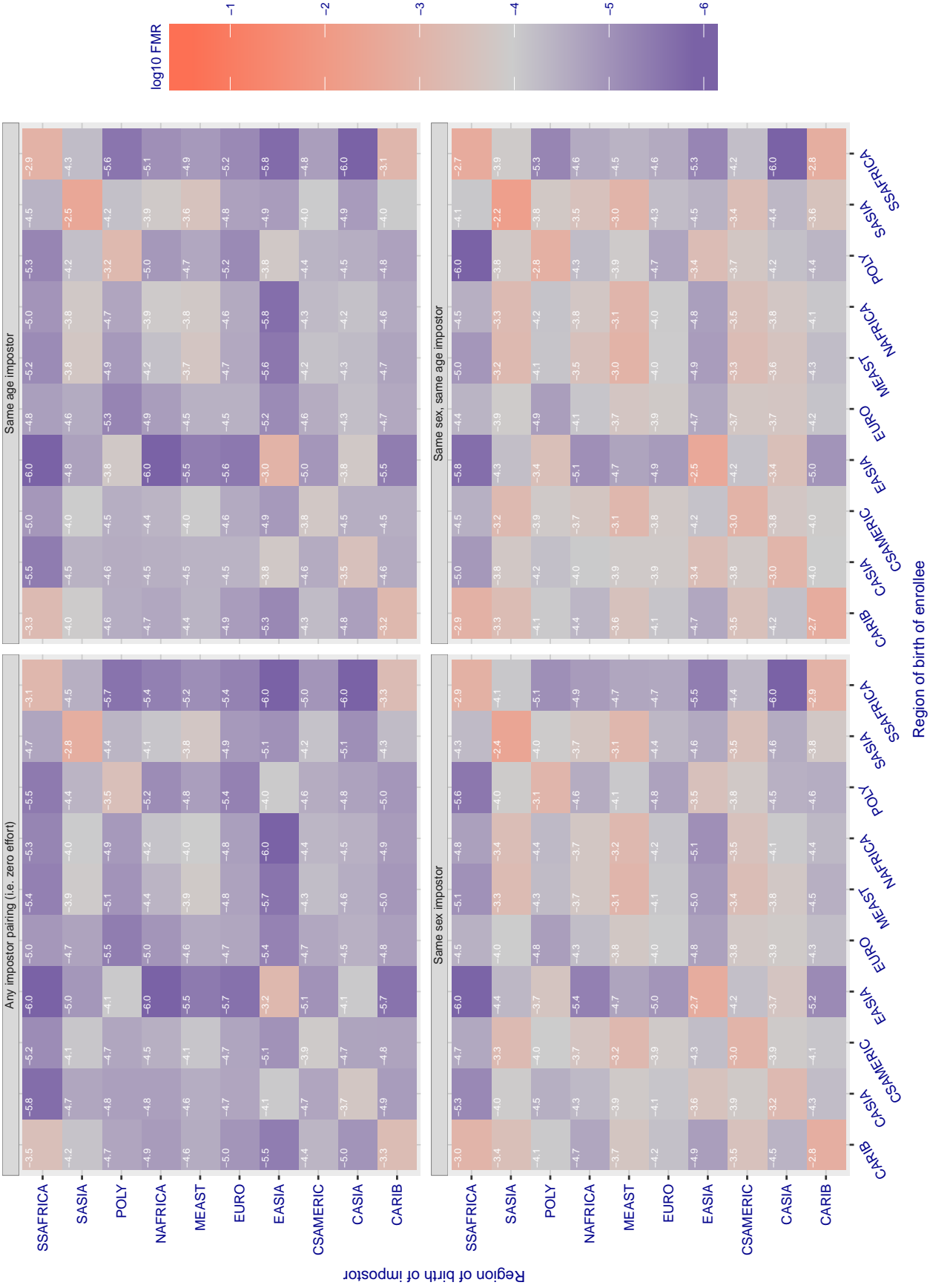


Figure 29: For algorithm ayonix-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.681$ for algorithm camvi_001, giving $FMR(T) = 0.0001$ globally.

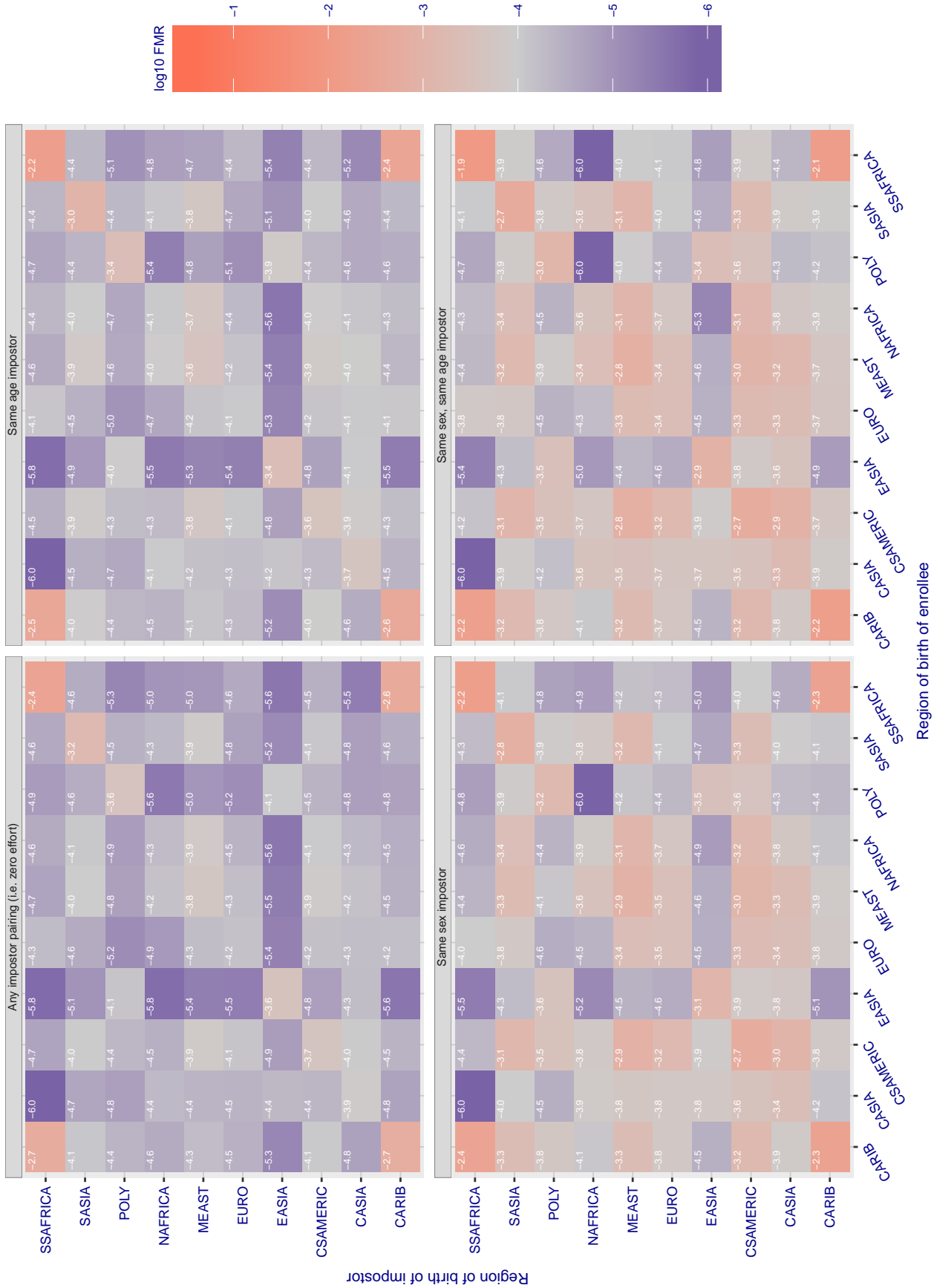


Figure 30: For algorithm camvi-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 3564.000$ for algorithm cogent_000 , giving $\text{FMR}(T) = 0.0001$ globally.

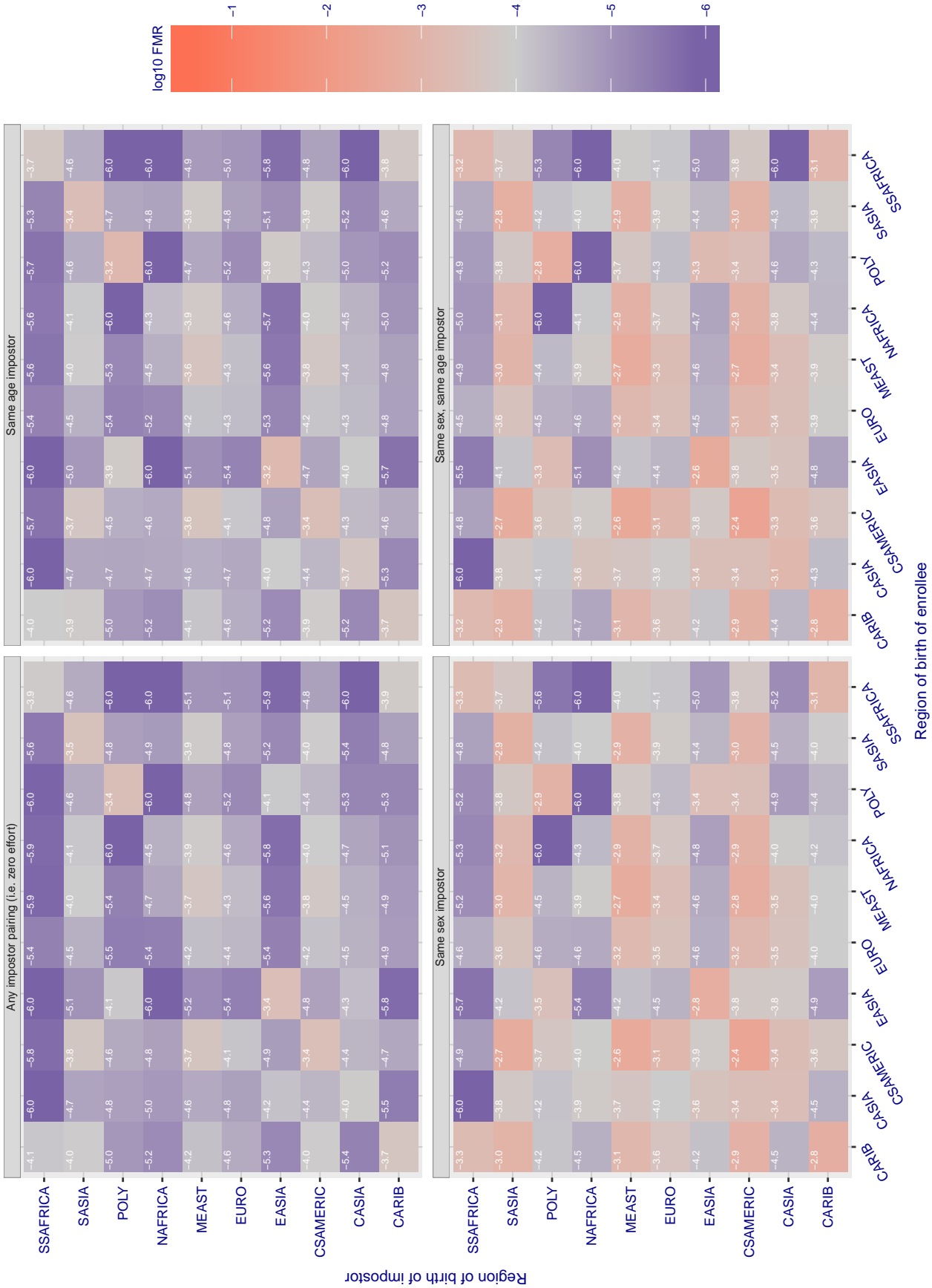


Figure 31: For algorithm cogent_000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} \text{FMR}$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.762$ for algorithm cyberextruder_001, giving $FMR(T) = 0.0001$ globally.

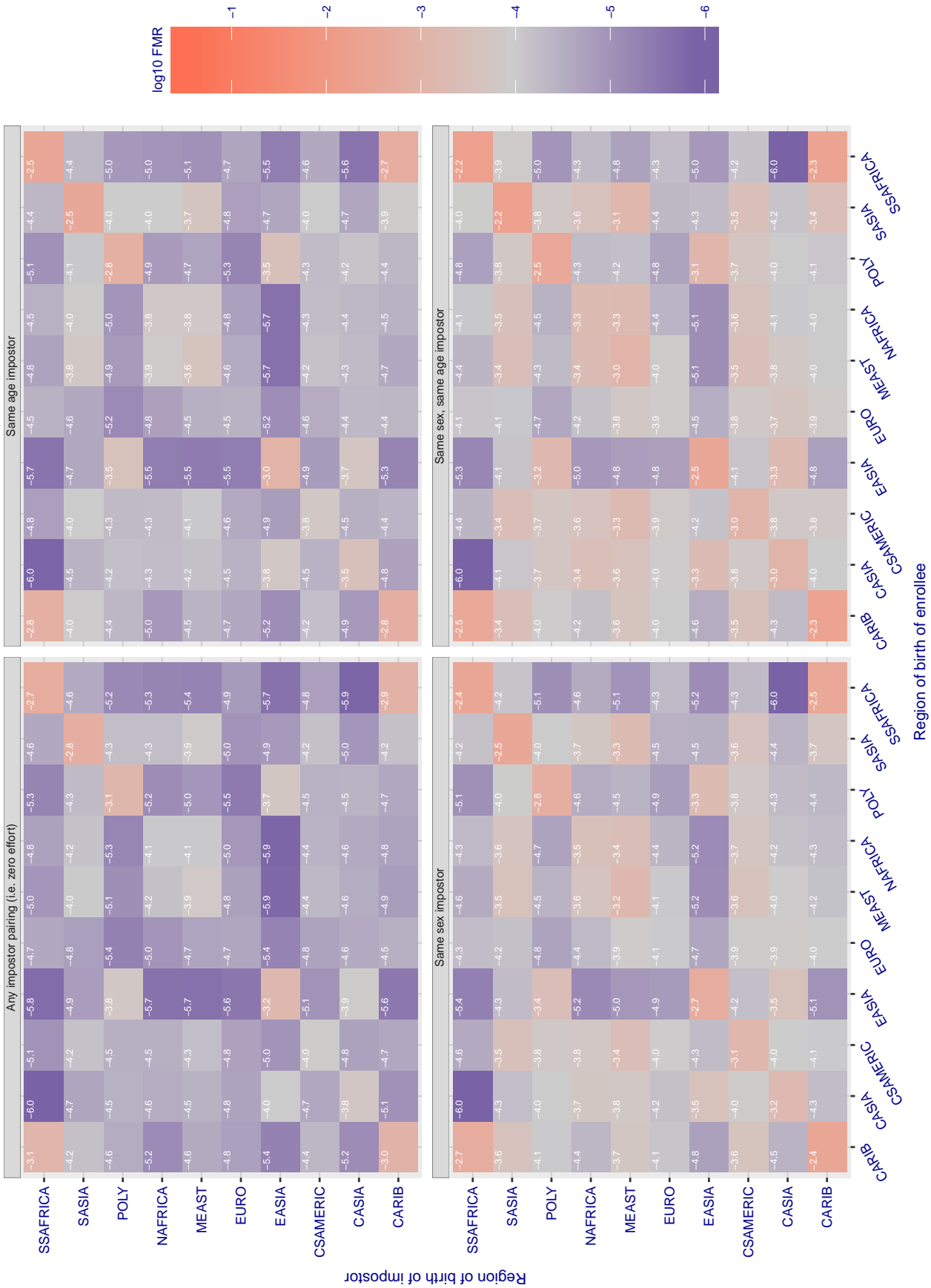


Figure 32: For algorithm cyberextruder-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 84.718$ for algorithm dermalog_003, giving $FMR(T) = 0.0001$ globally.

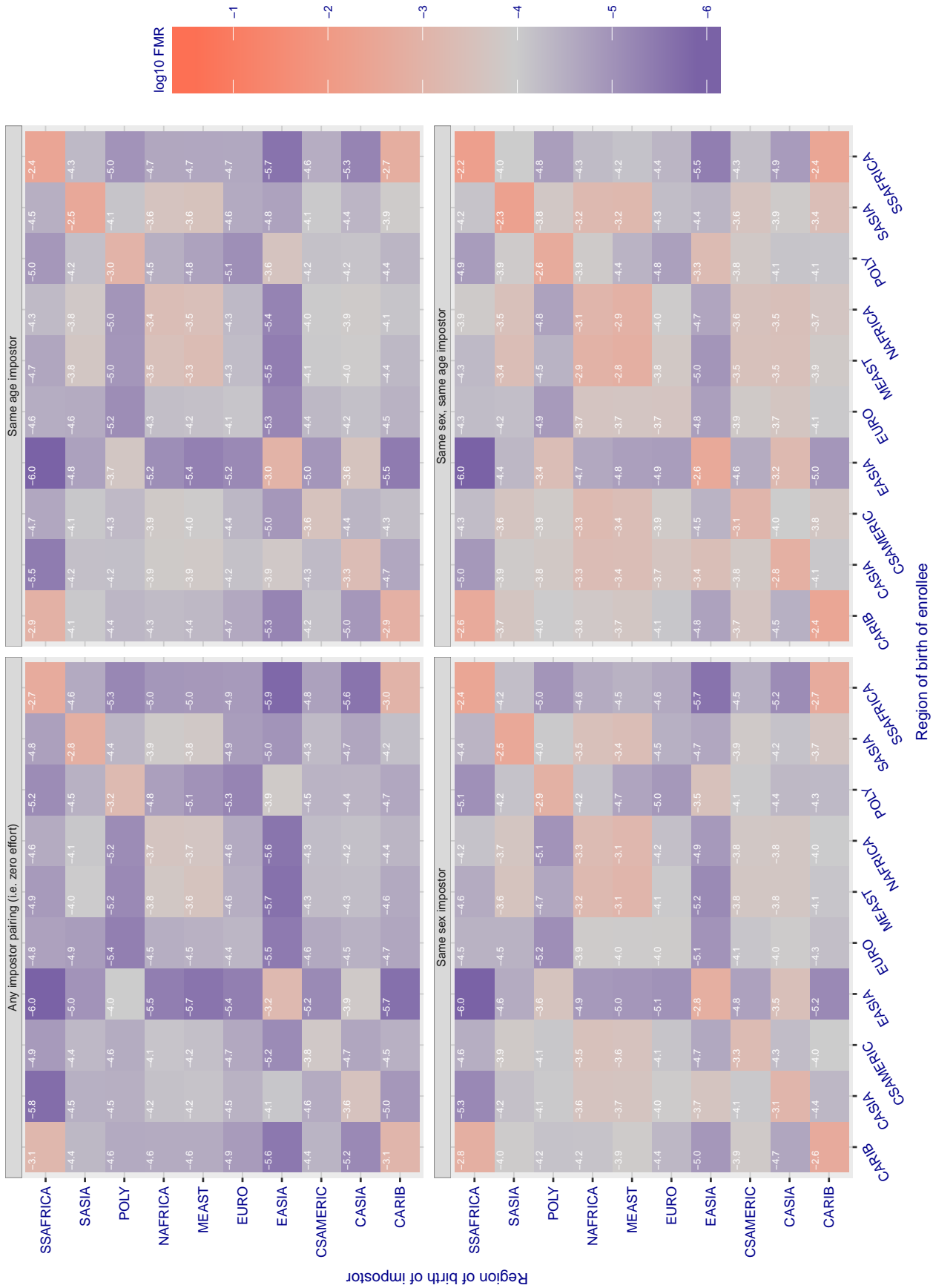


Figure 33: For algorithm dermalog-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 81.959$ for algorithm dermalog_004, giving $FMR(T) = 0.0001$ globally.

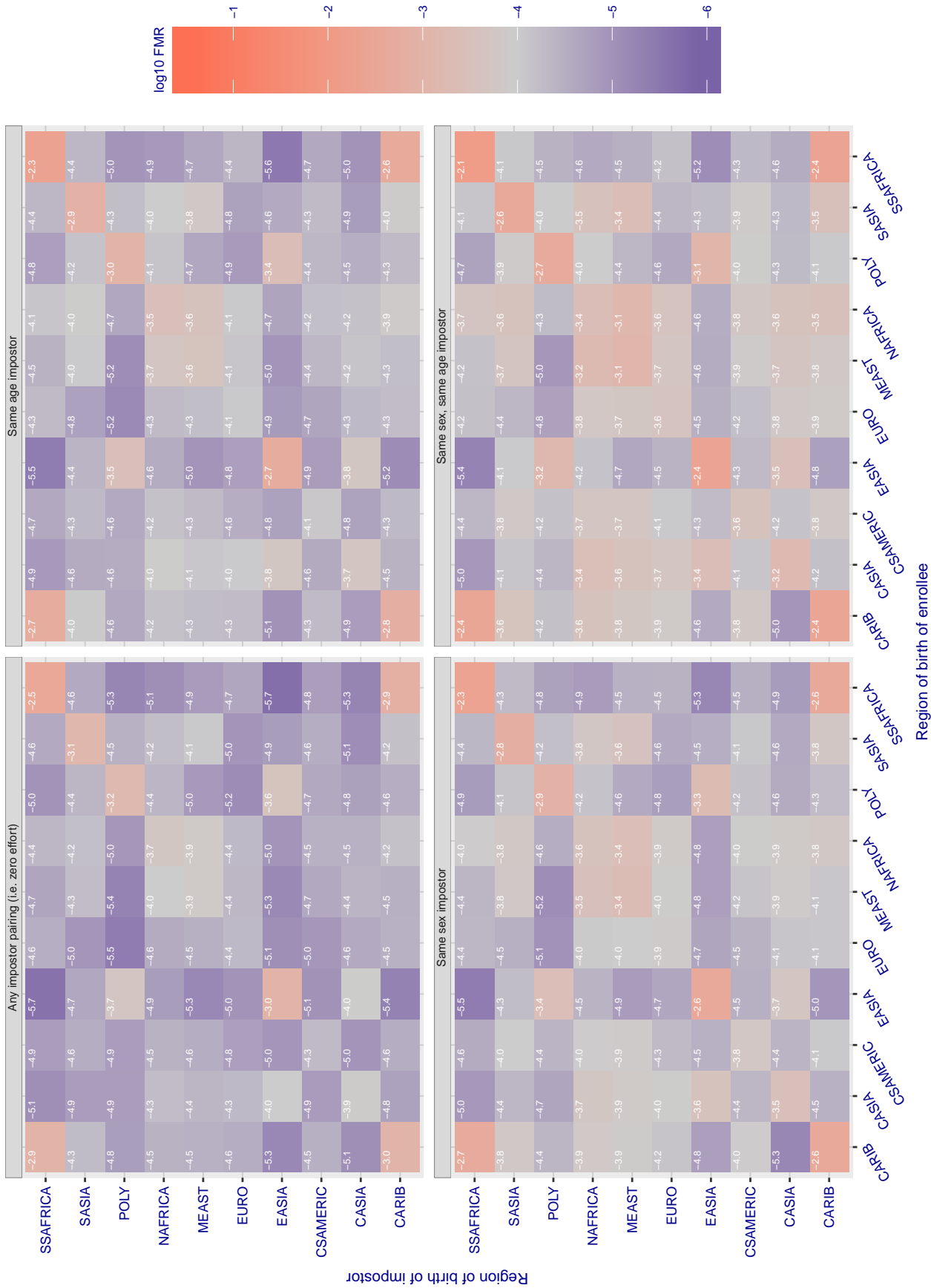


Figure 34: For algorithm dermalog-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.646$ for algorithm digitalbarriers_000, giving $FMR(T) = 0.0001$ globally.

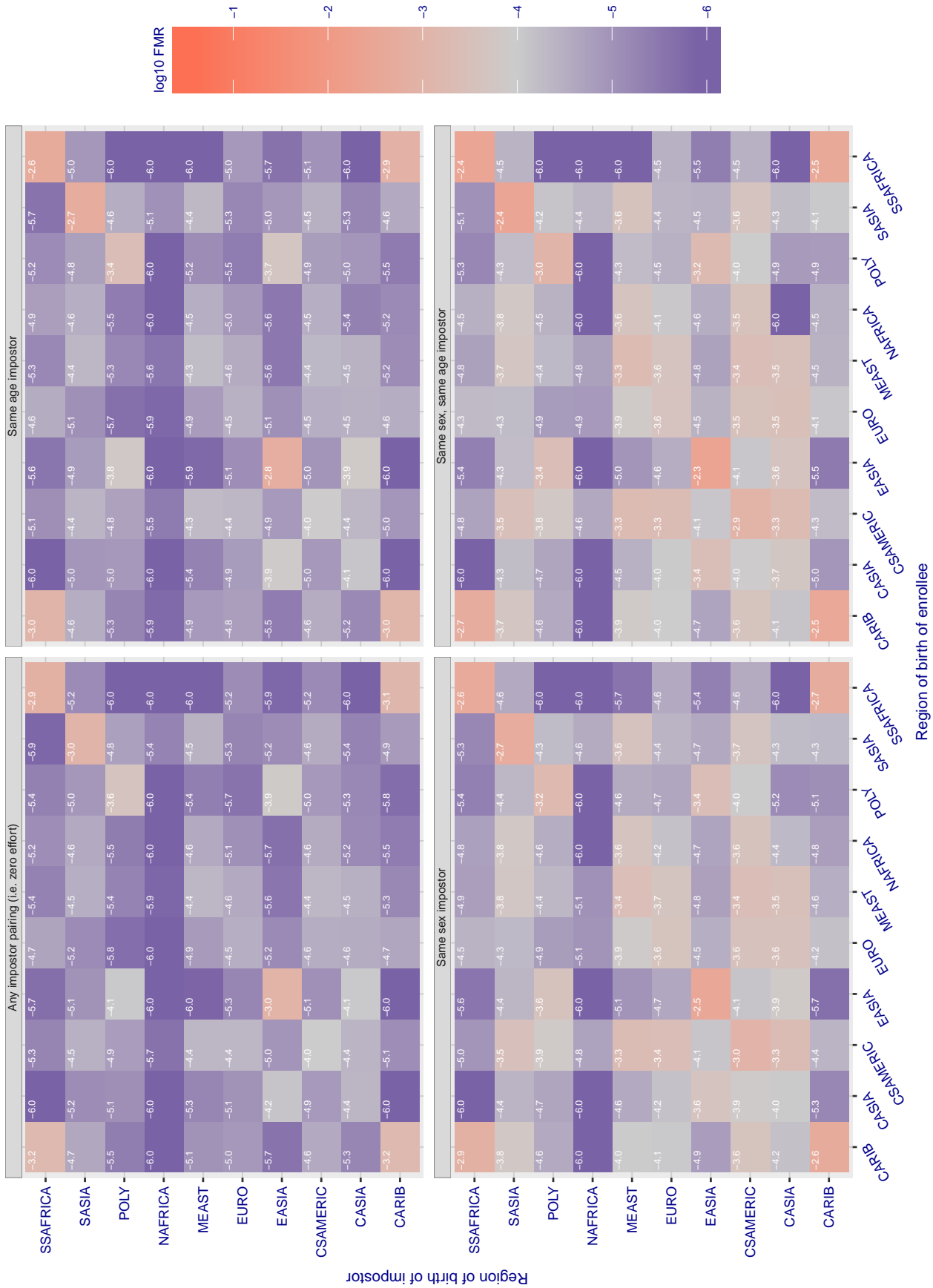


Figure 35: For algorithm digitalbarriers-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.700$ for algorithm digitalbarriers_001, giving $FMR(T) = 0.0001$ globally.

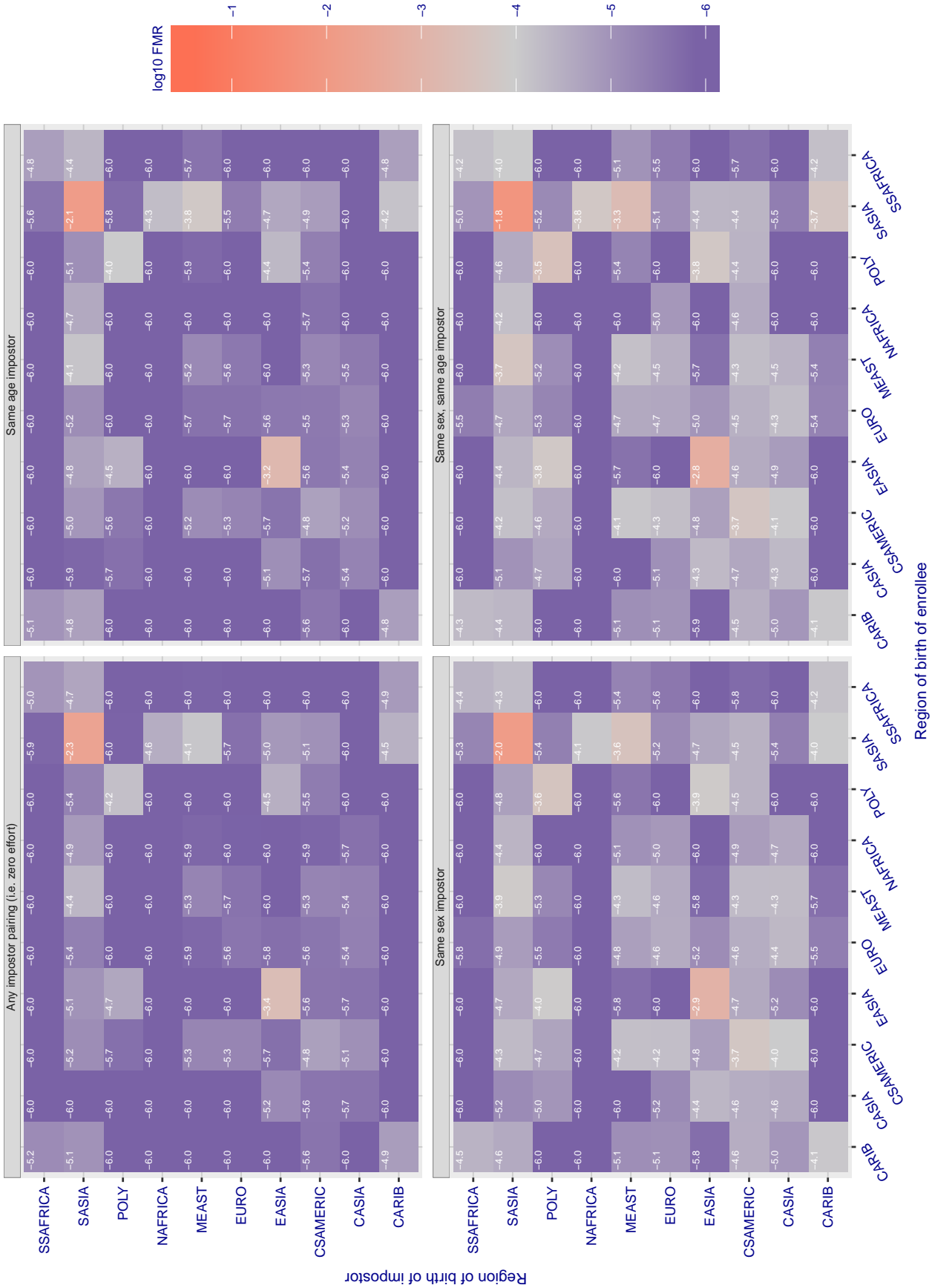


Figure 36: For algorithm digitalbarriers-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.798$ for algorithm fdu_000 , giving $\text{FMR}(T) = 0.0001$ globally.

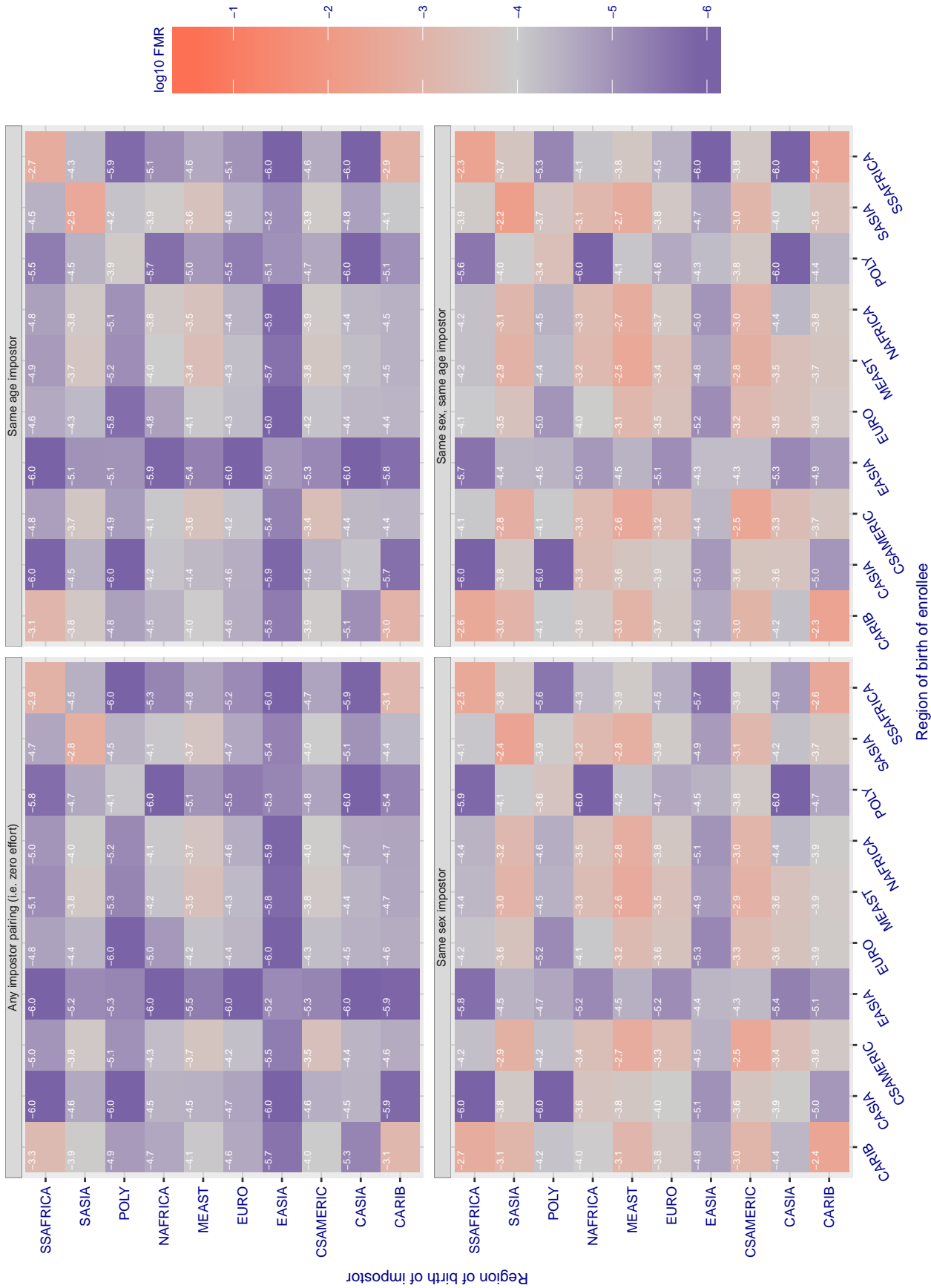


Figure 37: For algorithm fdu_000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.850$ for algorithm fdu_001 , giving $\text{FMR}(T) = 0.0001$ globally.

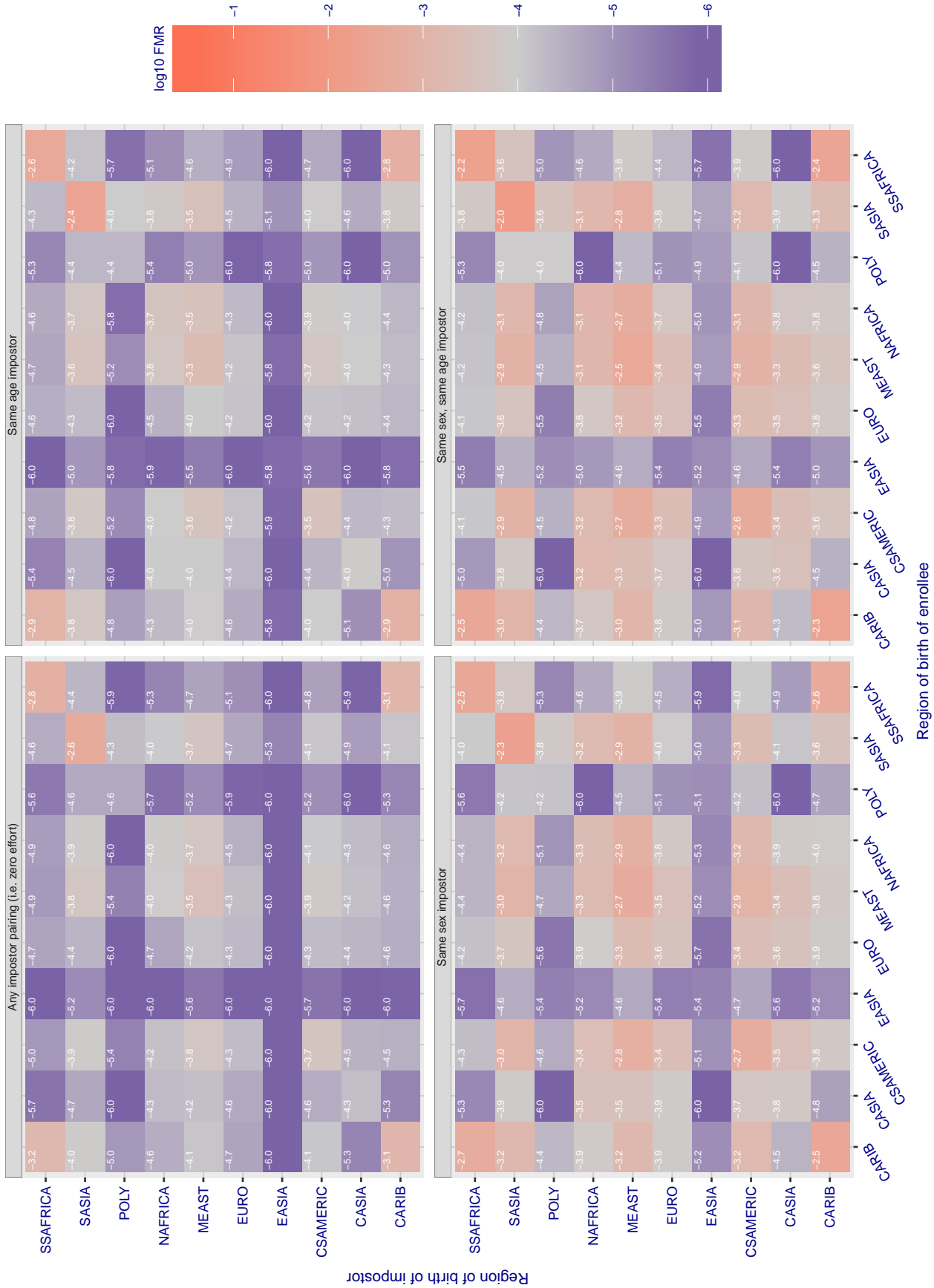


Figure 38: For algorithm fdu_001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it gives the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} \text{FMR}$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 2611.000$ for algorithm id3_001, giving $FMR(T) = 0.0001$ globally.

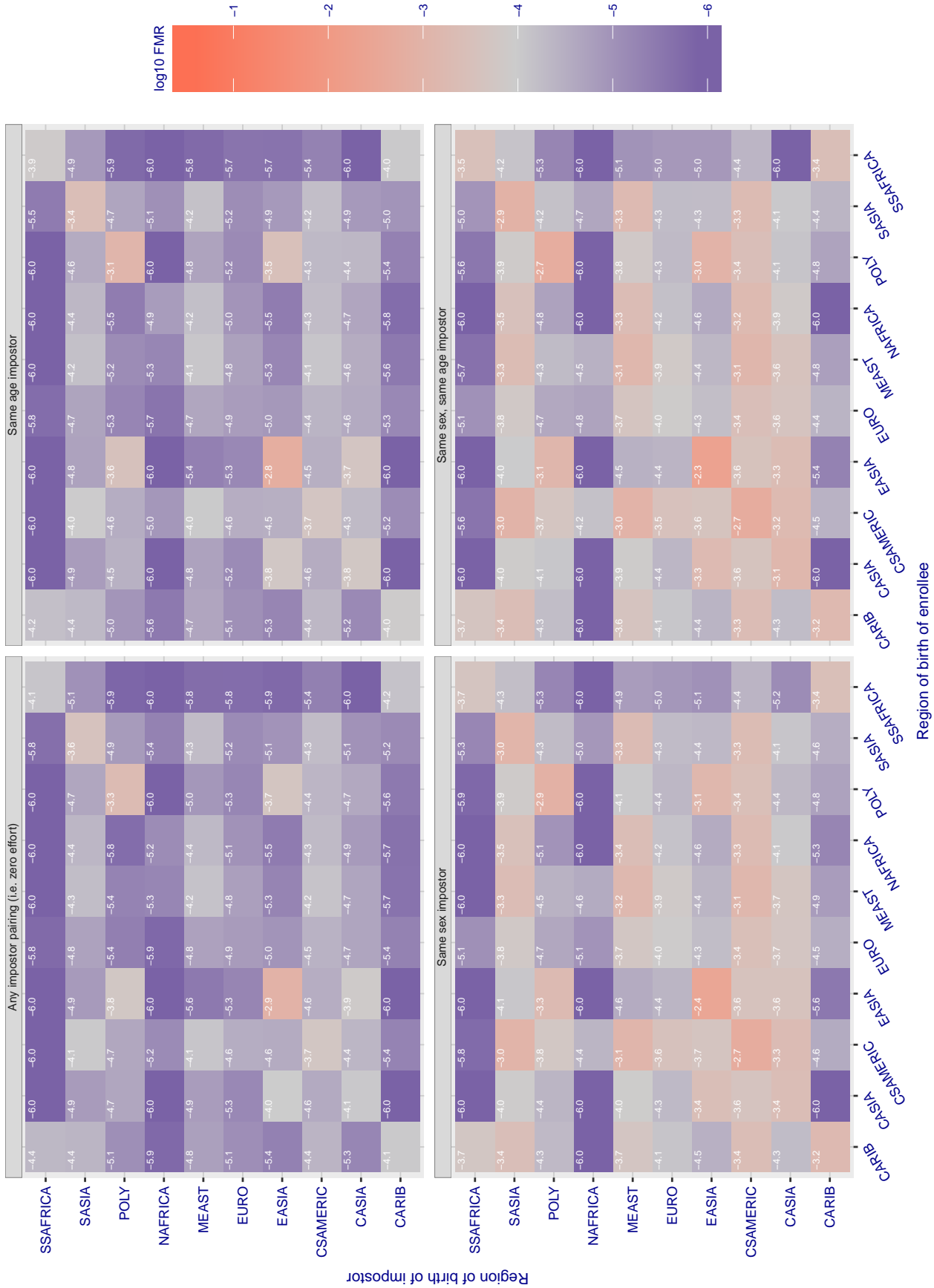


Figure 39: For algorithm id3-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 2649.000$ for algorithm id3_002, giving $FMR(T) = 0.0001$ globally.

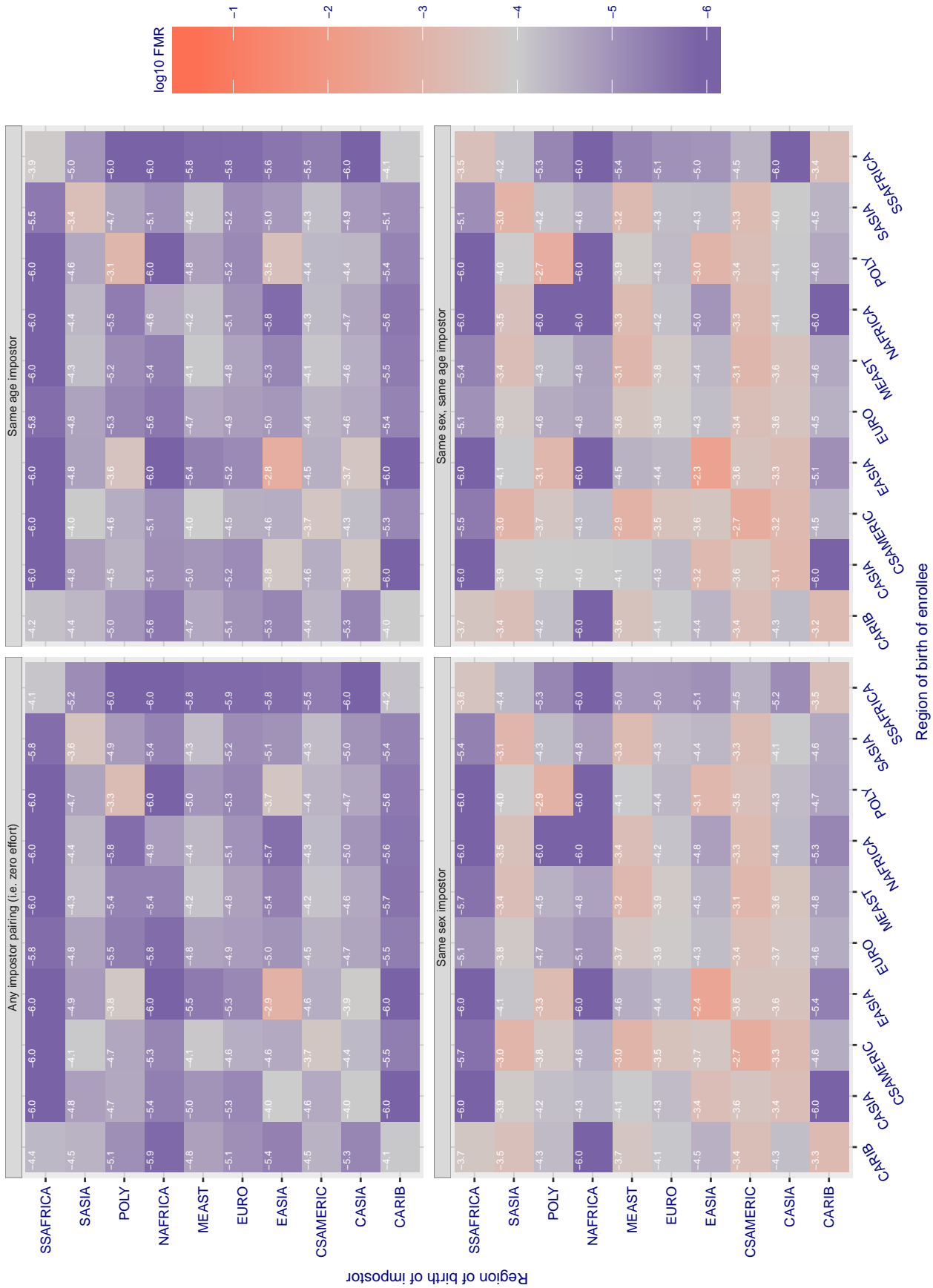


Figure 40: For algorithm id3-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 58.258$ for algorithm innovatrics_000, giving $FMR(T) = 0.0001$ globally.

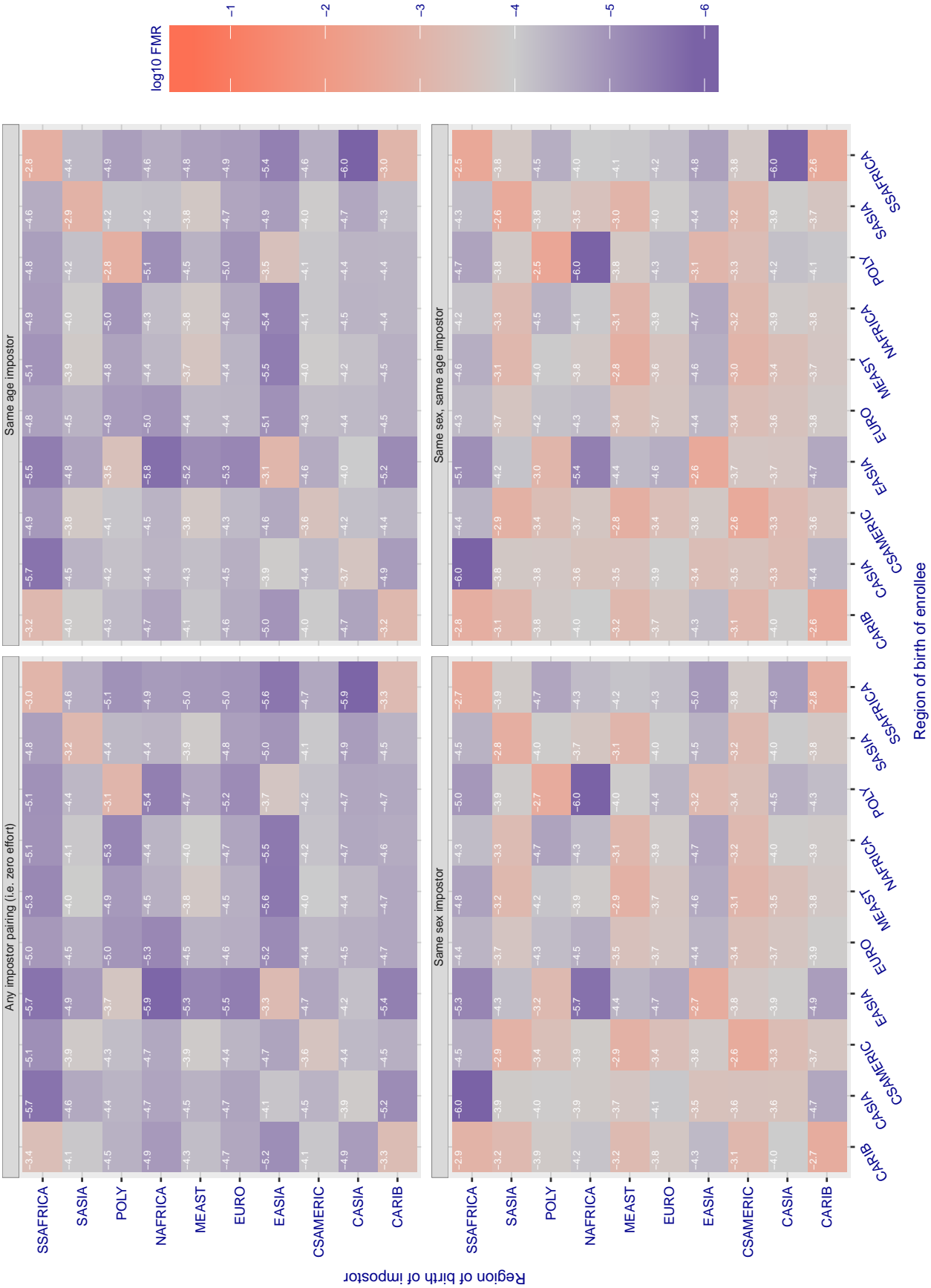


Figure 41: For algorithm innovatrics-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 54.156$ for algorithm innovatrics_001, giving $FMR(T) = 0.0001$ globally.

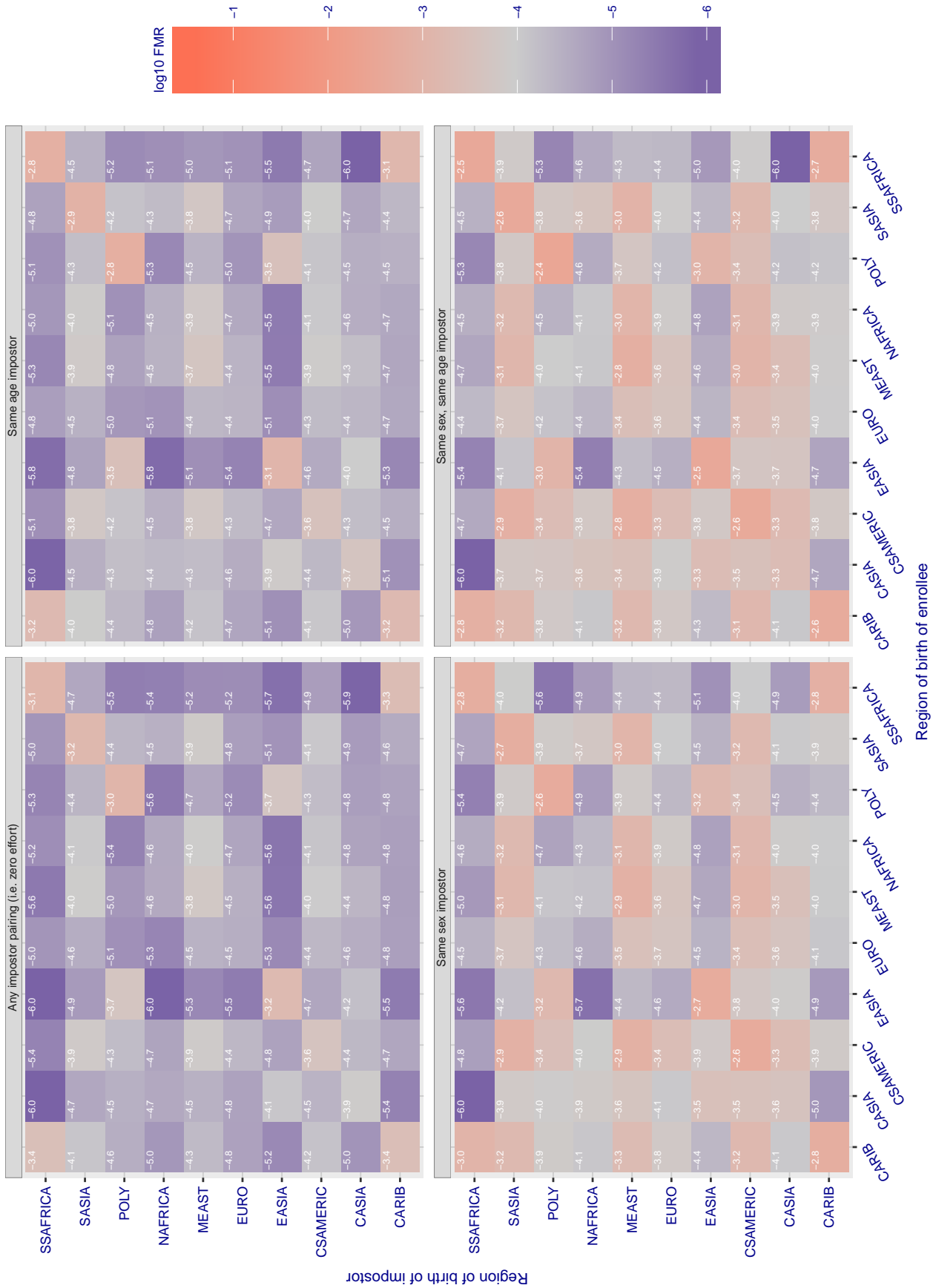


Figure 42: For algorithm innovatrics-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 49.664$ for algorithm intellivision_001, giving $FMR(T) = 0.0001$ globally.

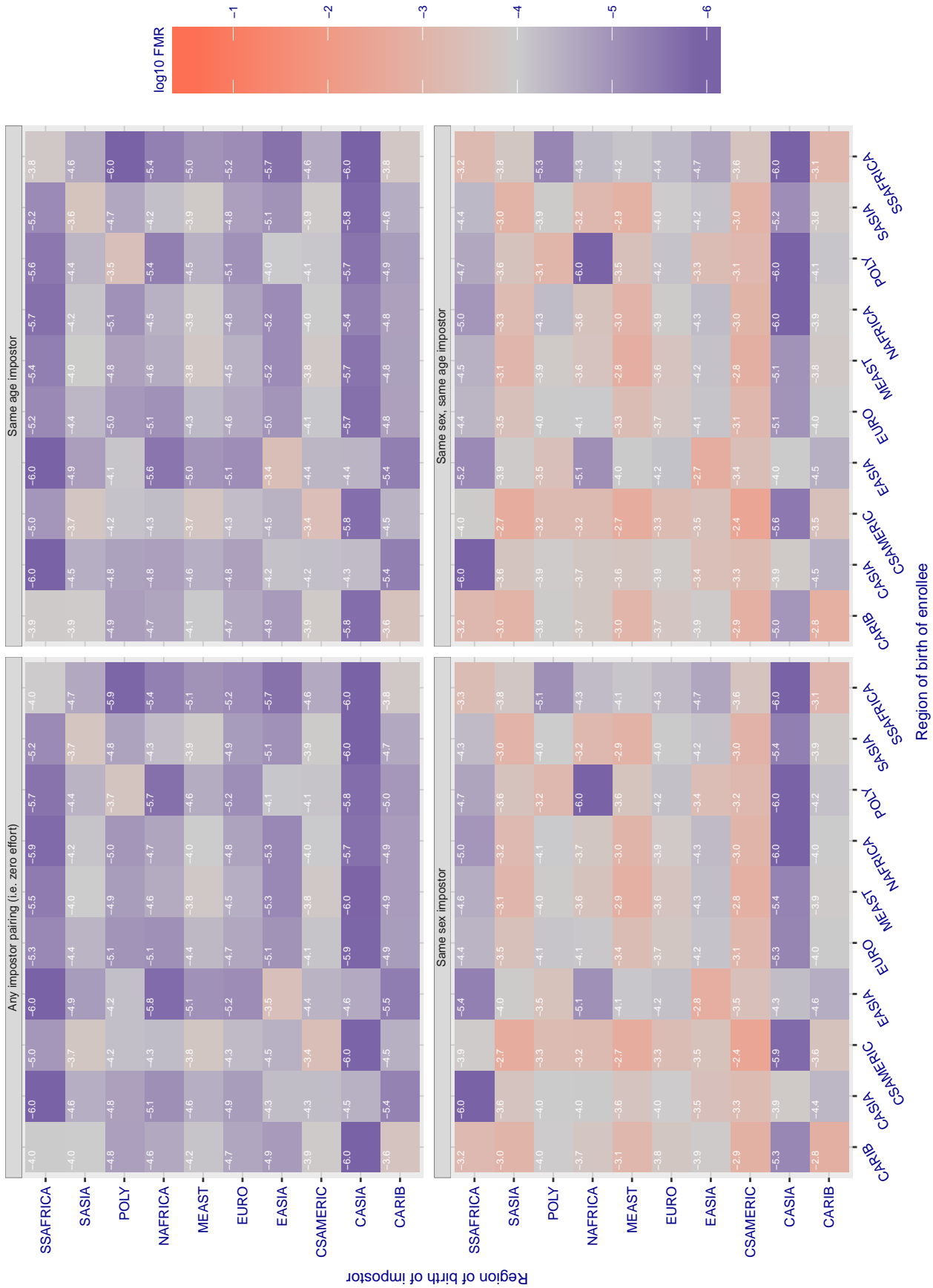


Figure 43: For algorithm intellivision-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 23.498$ for algorithm isityou_000, giving $FMR(T) = 0.0001$ globally.

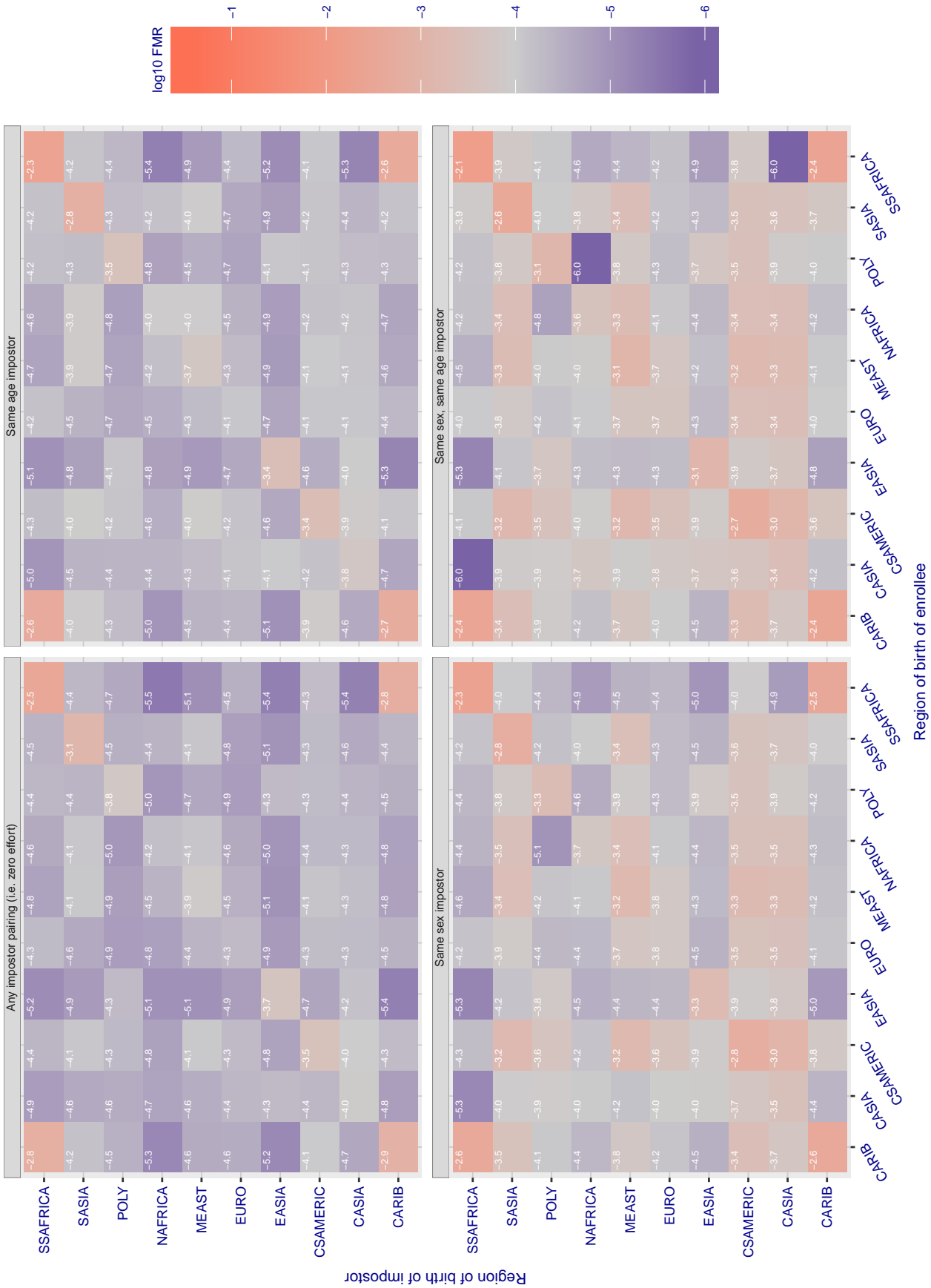


Figure 44: For algorithm isityou-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.782$ for algorithm isystems_000, giving $FMR(T) = 0.0001$ globally.

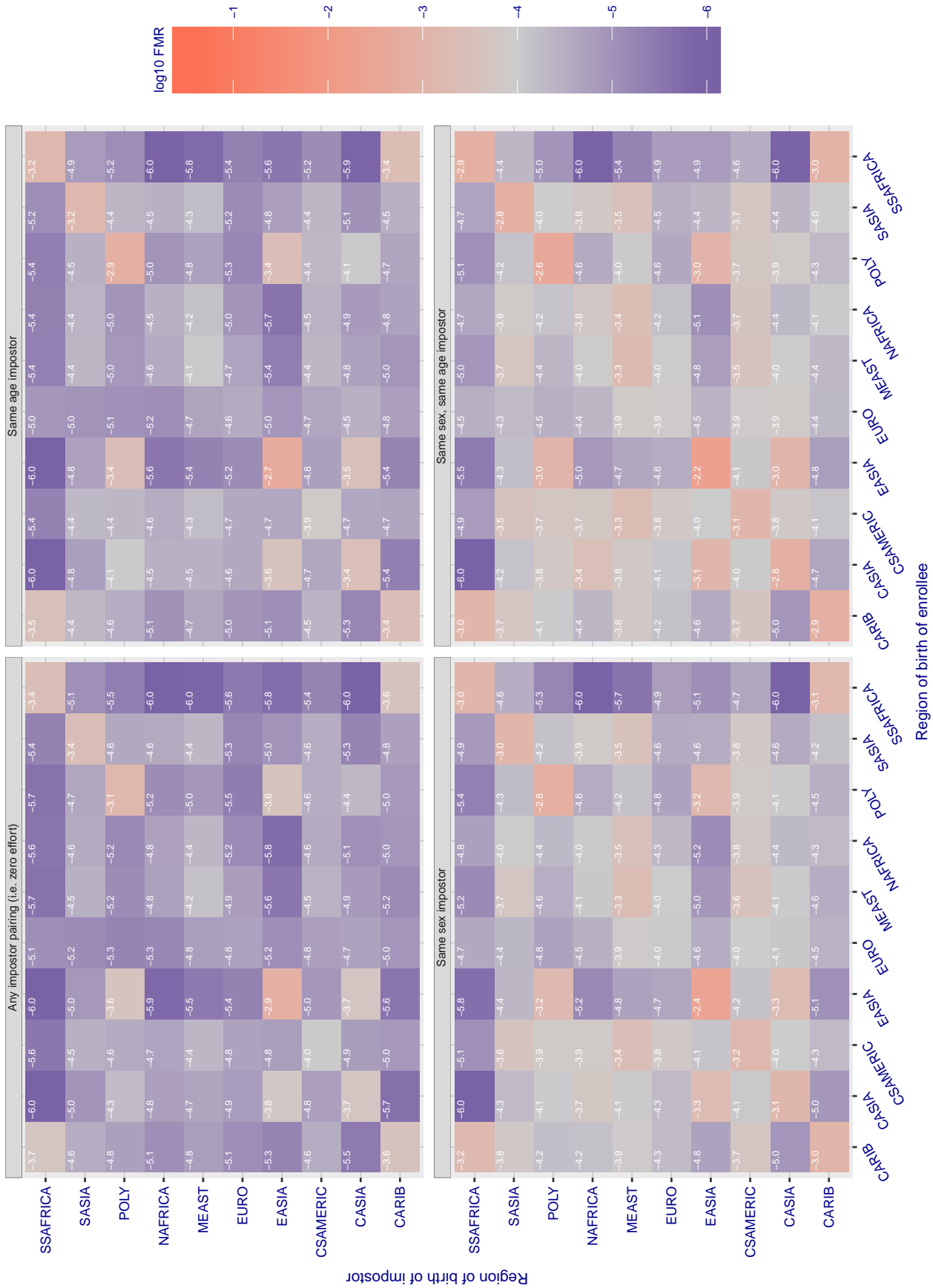


Figure 45: For algorithm isystems-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 998.683$ for algorithm itmo_002, giving $FMR(T) = 0.0001$ globally.

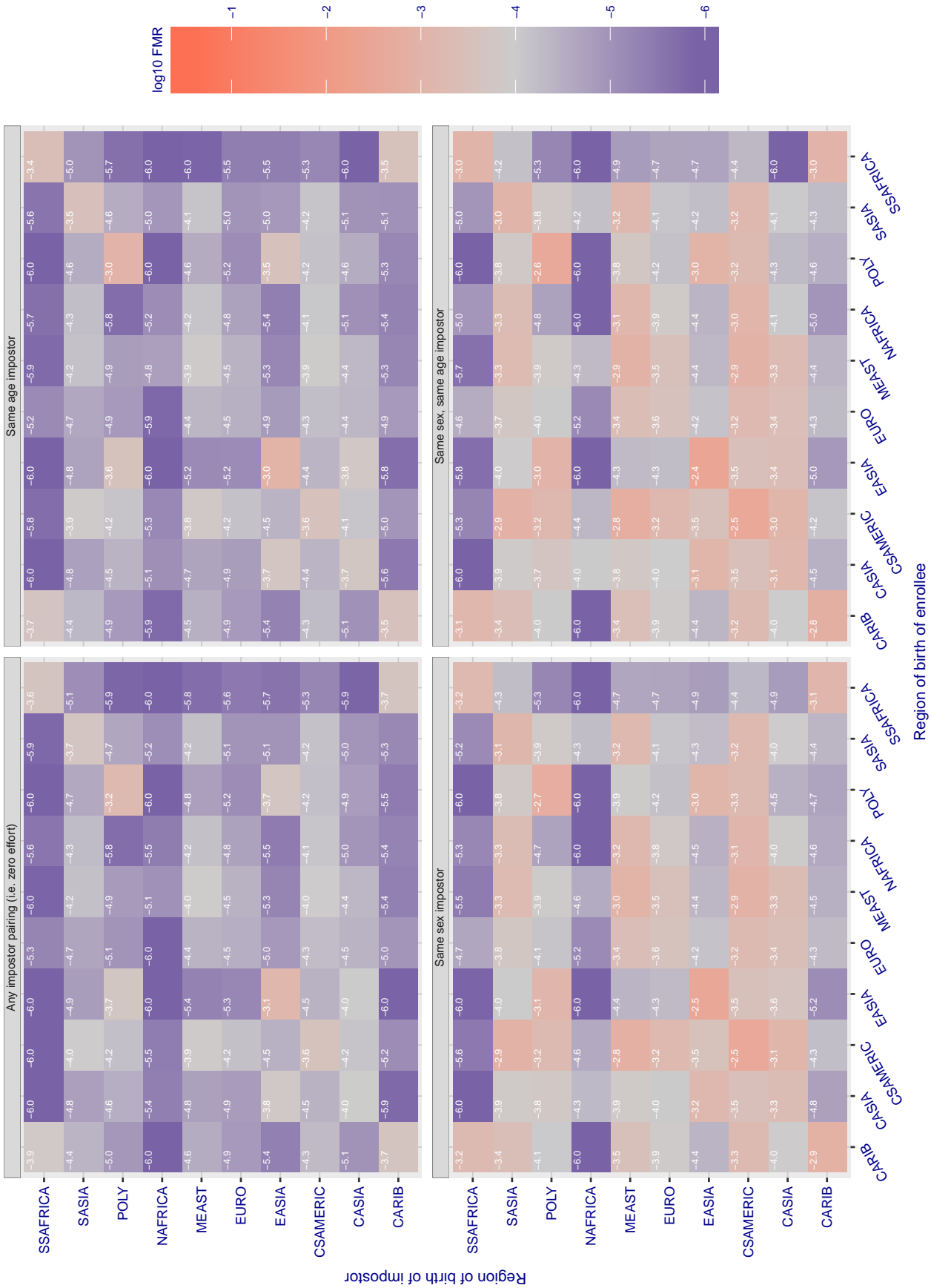


Figure 46: For algorithm itmo-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 3846.708$ for algorithm morpho_000, giving $FMR(T) = 0.0001$ globally.

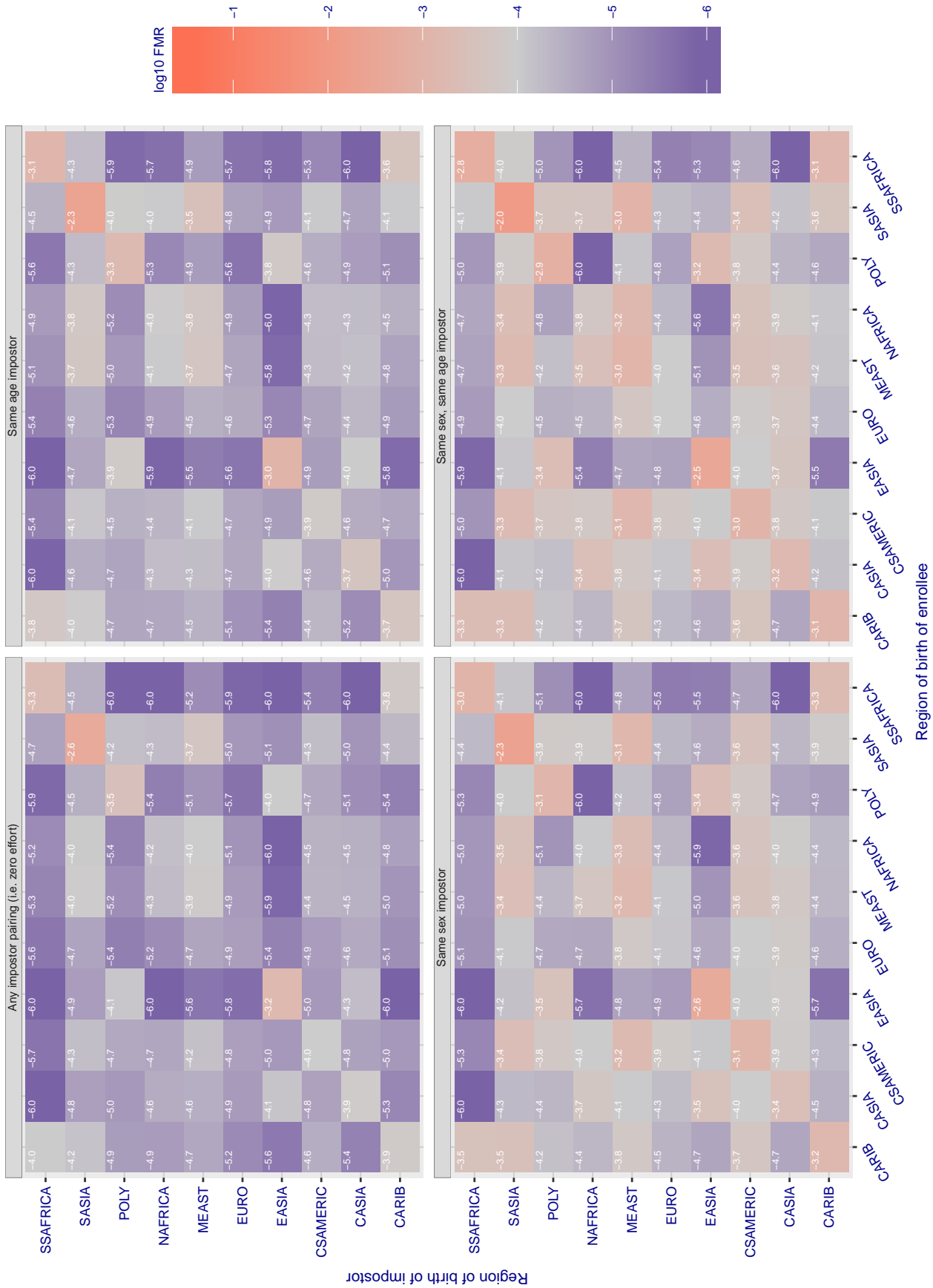


Figure 47: For algorithm morpho-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 3801.880$ for algorithm morpho_002, giving $FMR(T) = 0.0001$ globally.

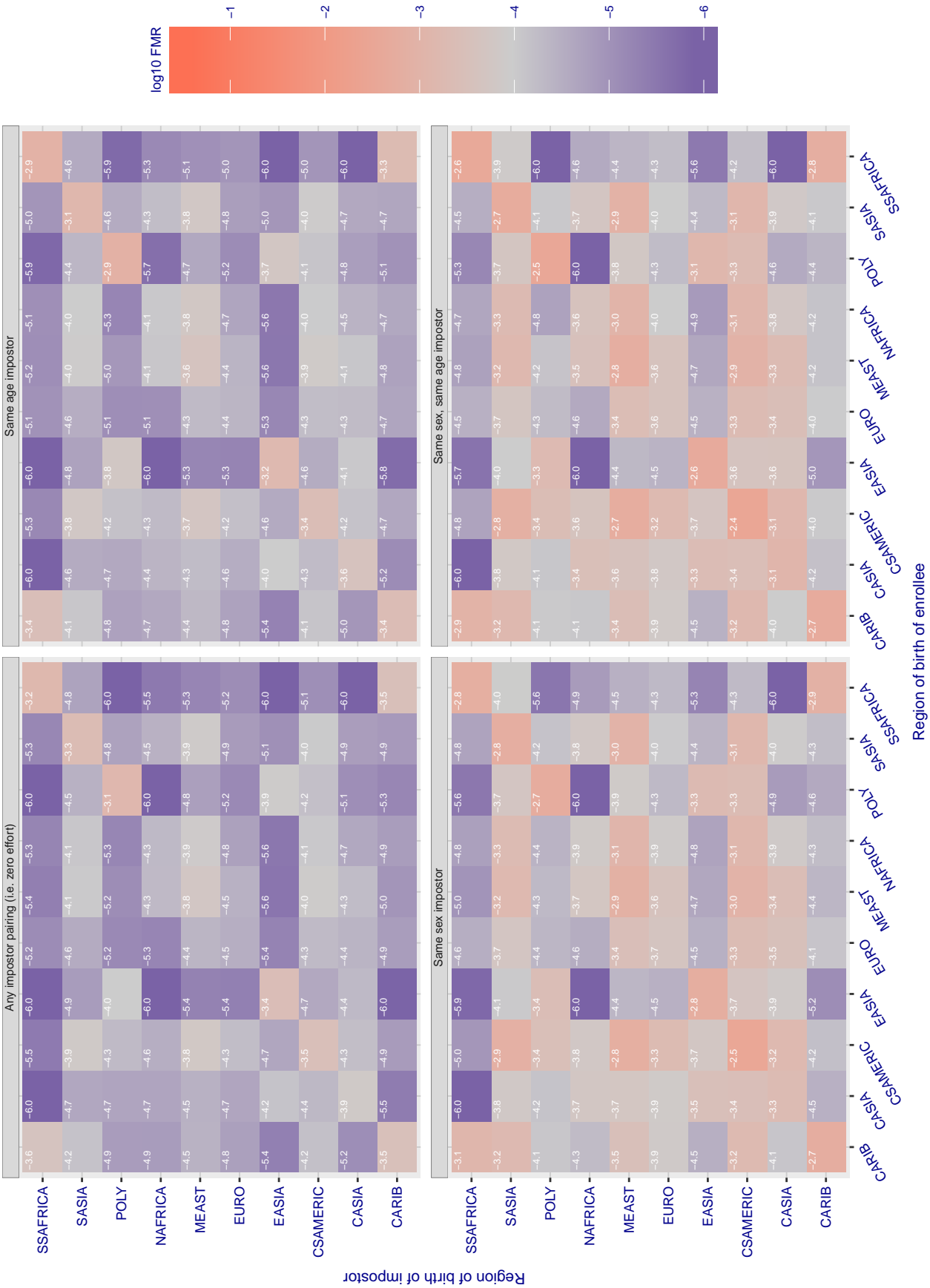


Figure 48: For algorithm morpho-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 45.600$ for algorithm neurotechnology_001, giving $FMR(T) = 0.0001$ globally.

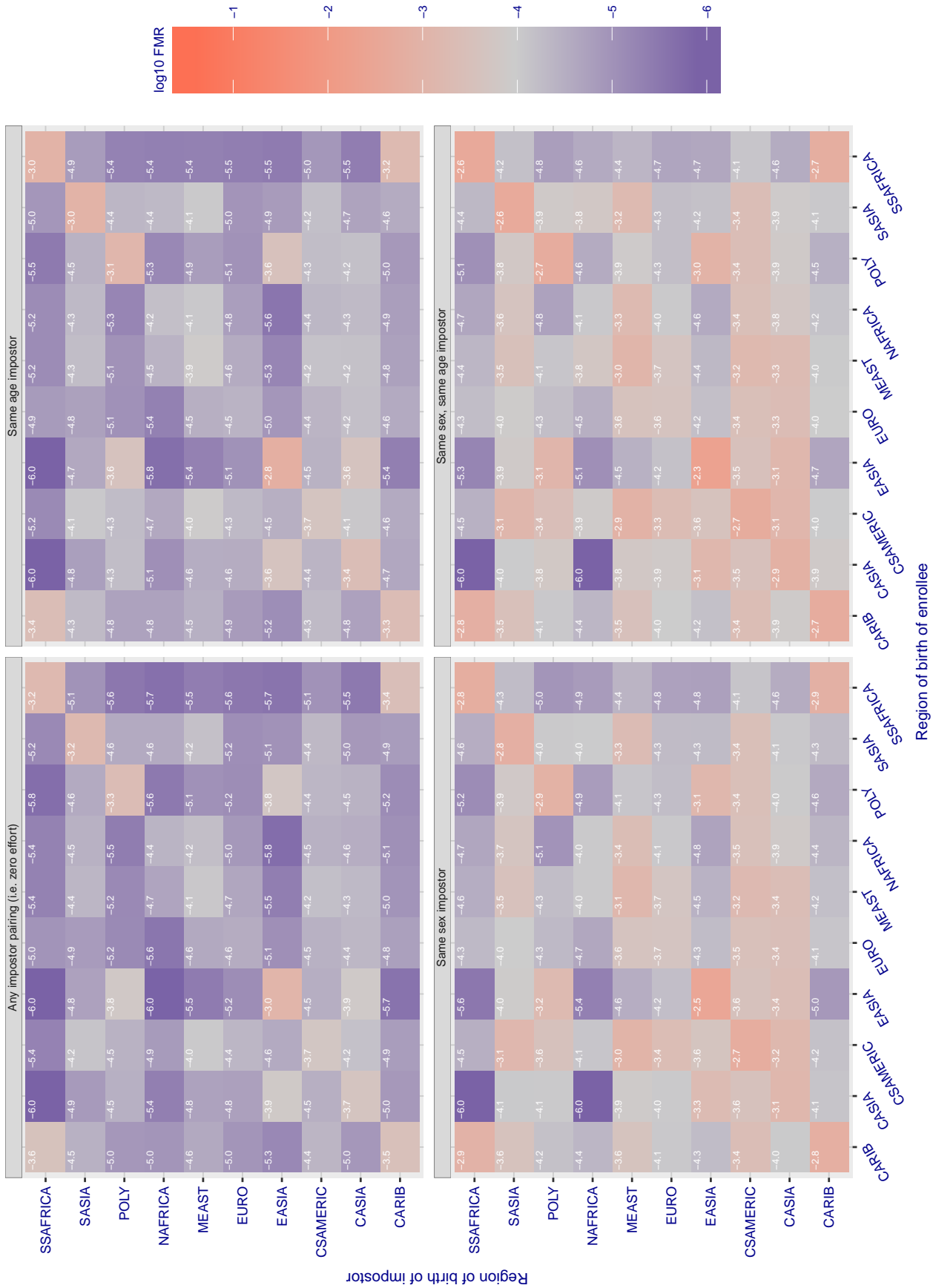


Figure 49: For algorithm neurotechnology-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 43.590$ for algorithm neurotechnology_002, giving $FMR(T) = 0.0001$ globally.

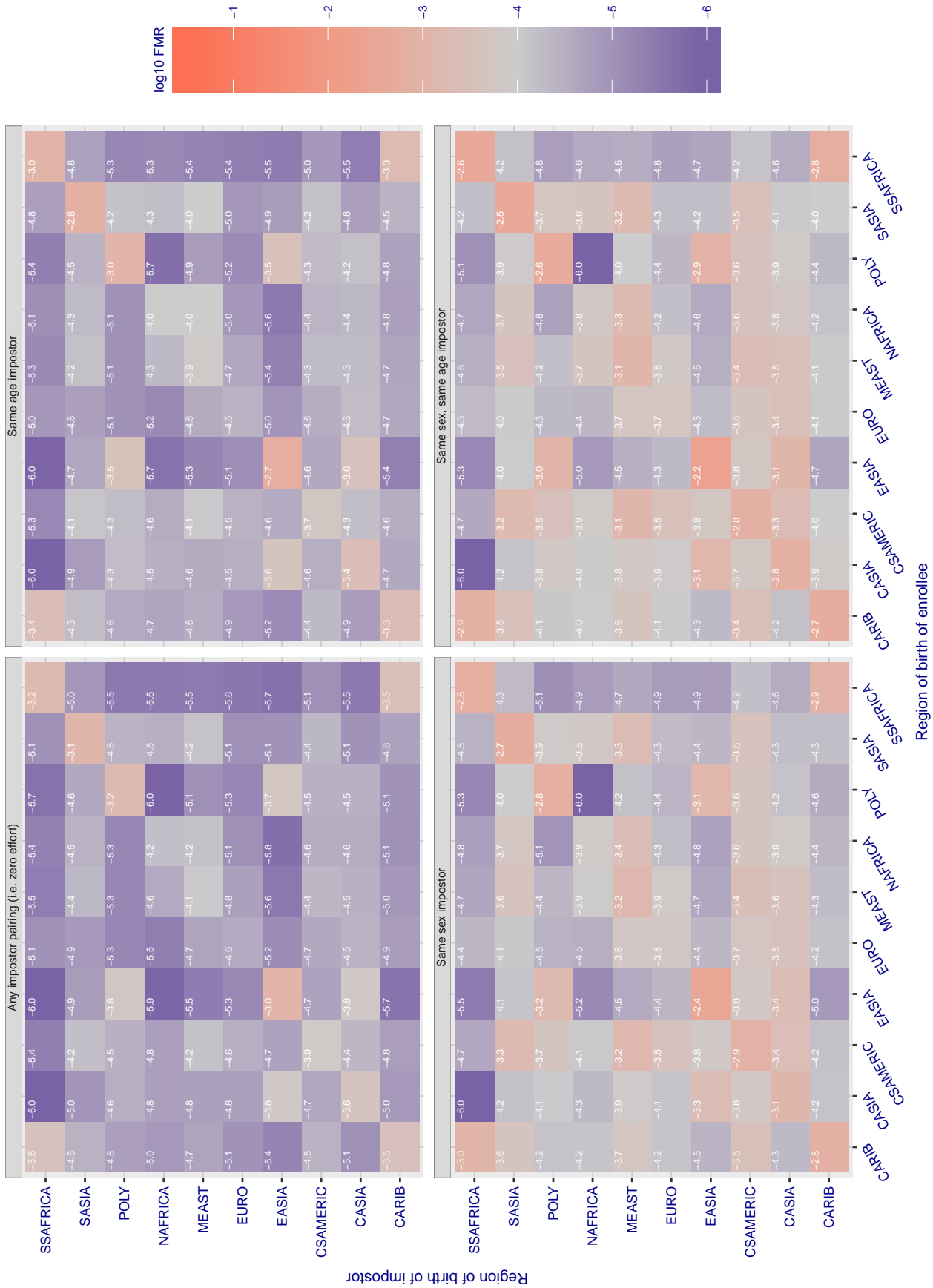


Figure 50: For algorithm neurotechnology-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = -0.660$ for algorithm noblis_000, giving $FMR(T) = 0.0001$ globally.

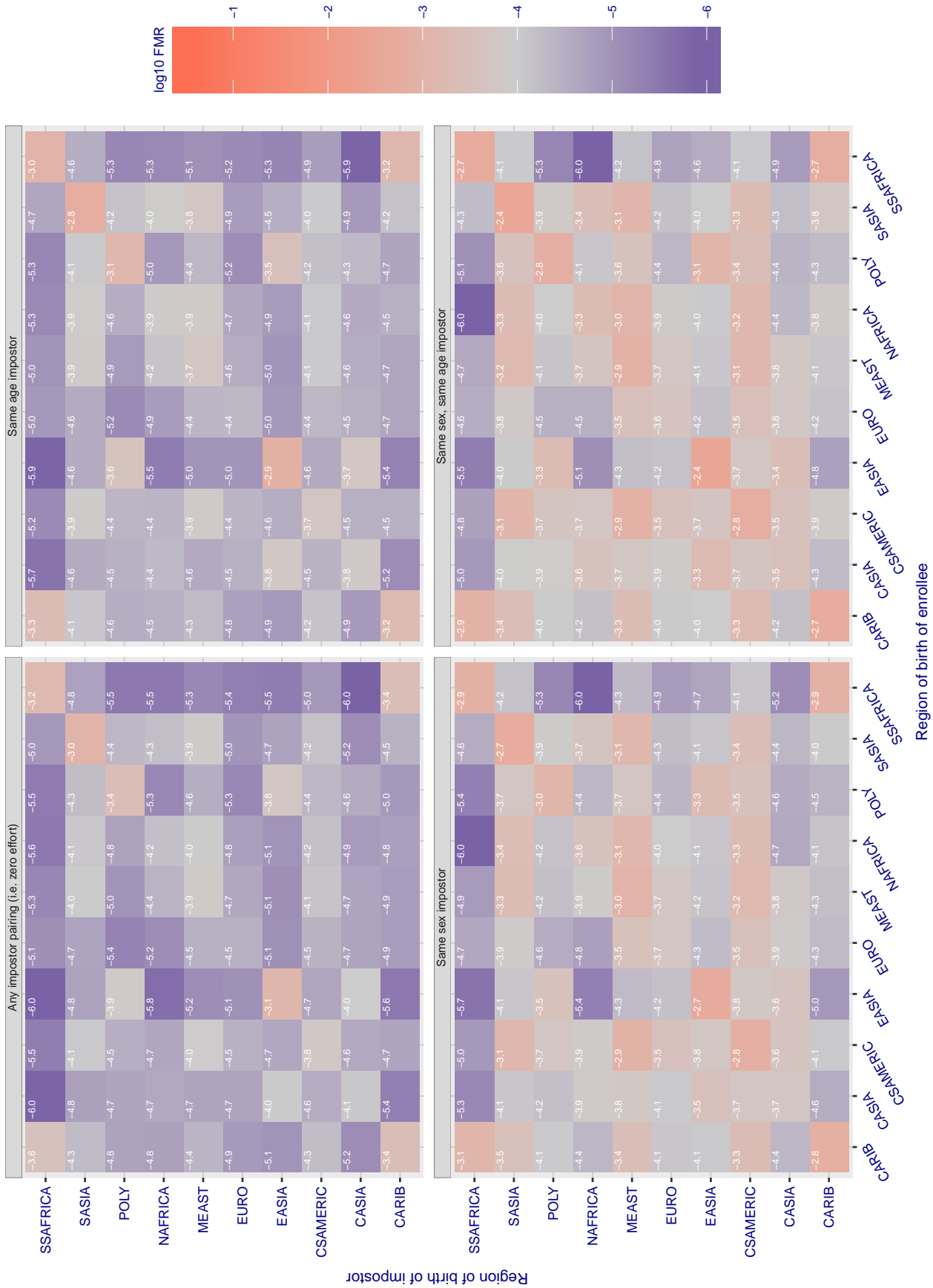


Figure 51: For algorithm noblis-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.099$ for algorithm ntechlab_002, giving $FMR(T) = 0.0001$ globally.

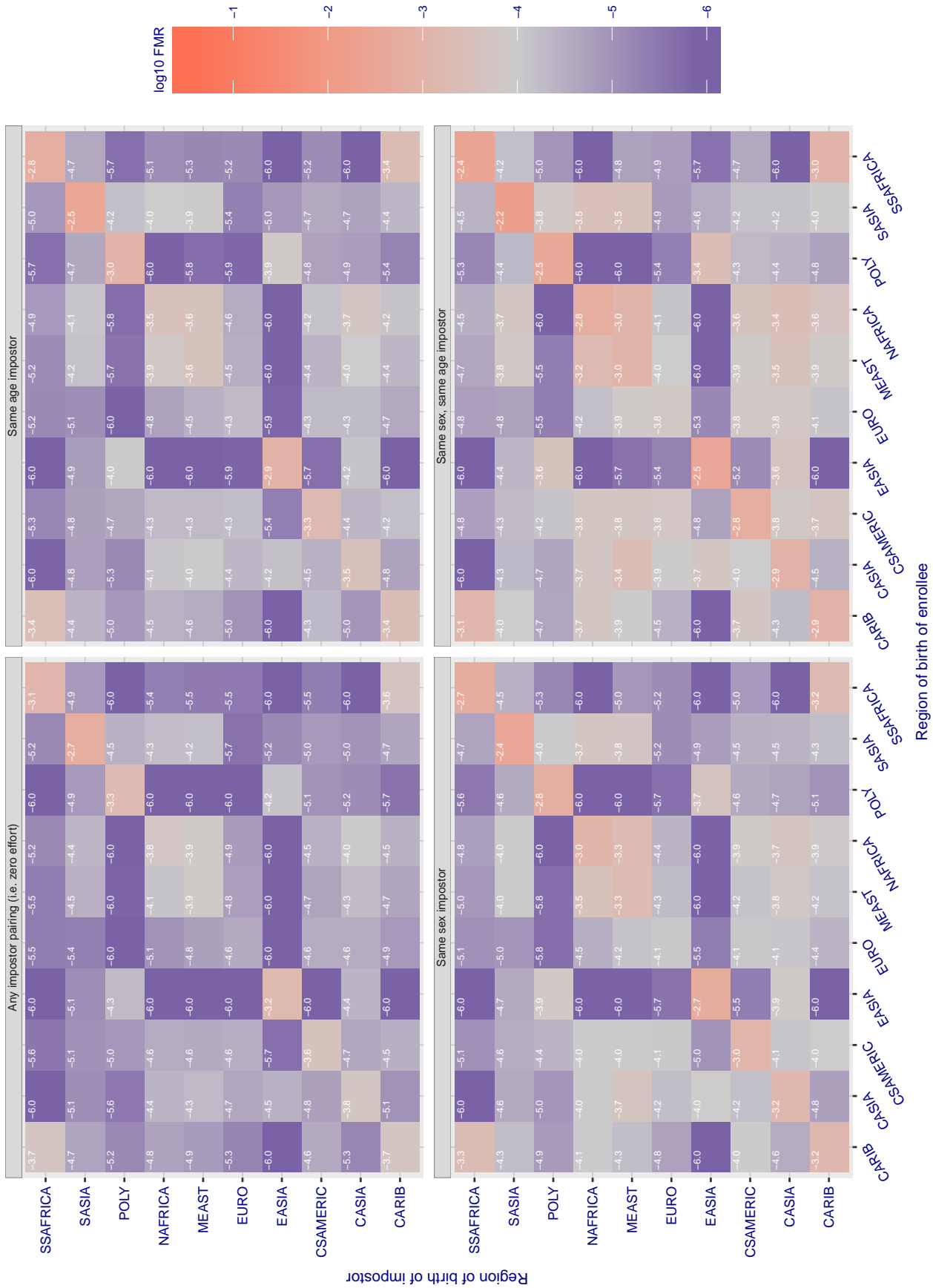


Figure 52: For algorithm ntechlab-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 3.759$ for algorithm ntechlab_003, giving $FMR(T) = 0.0001$ globally.

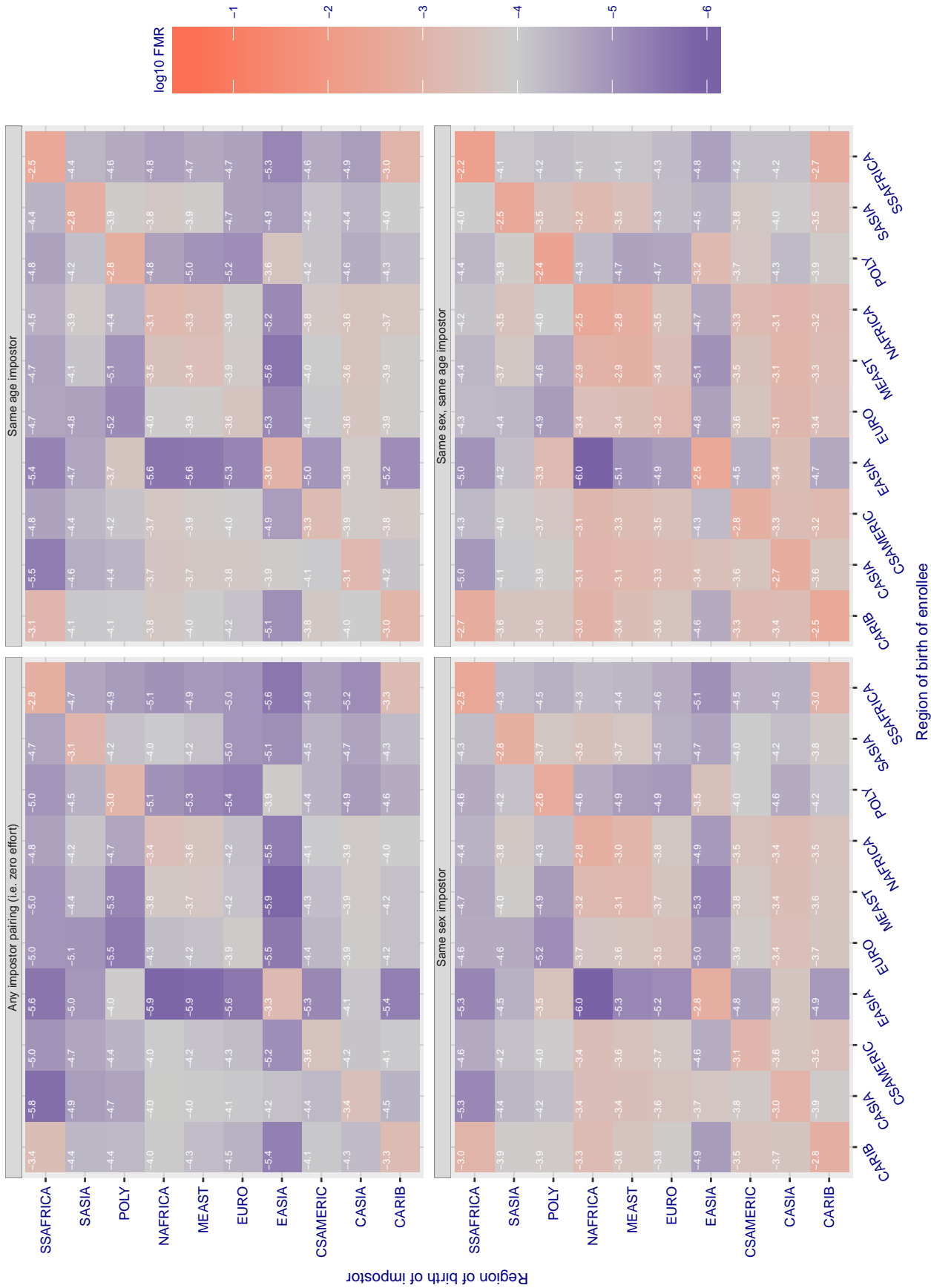


Figure 53: For algorithm ntechlab-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.839$ for algorithm pa_002, giving $FMR(T) = 0.0001$ globally.

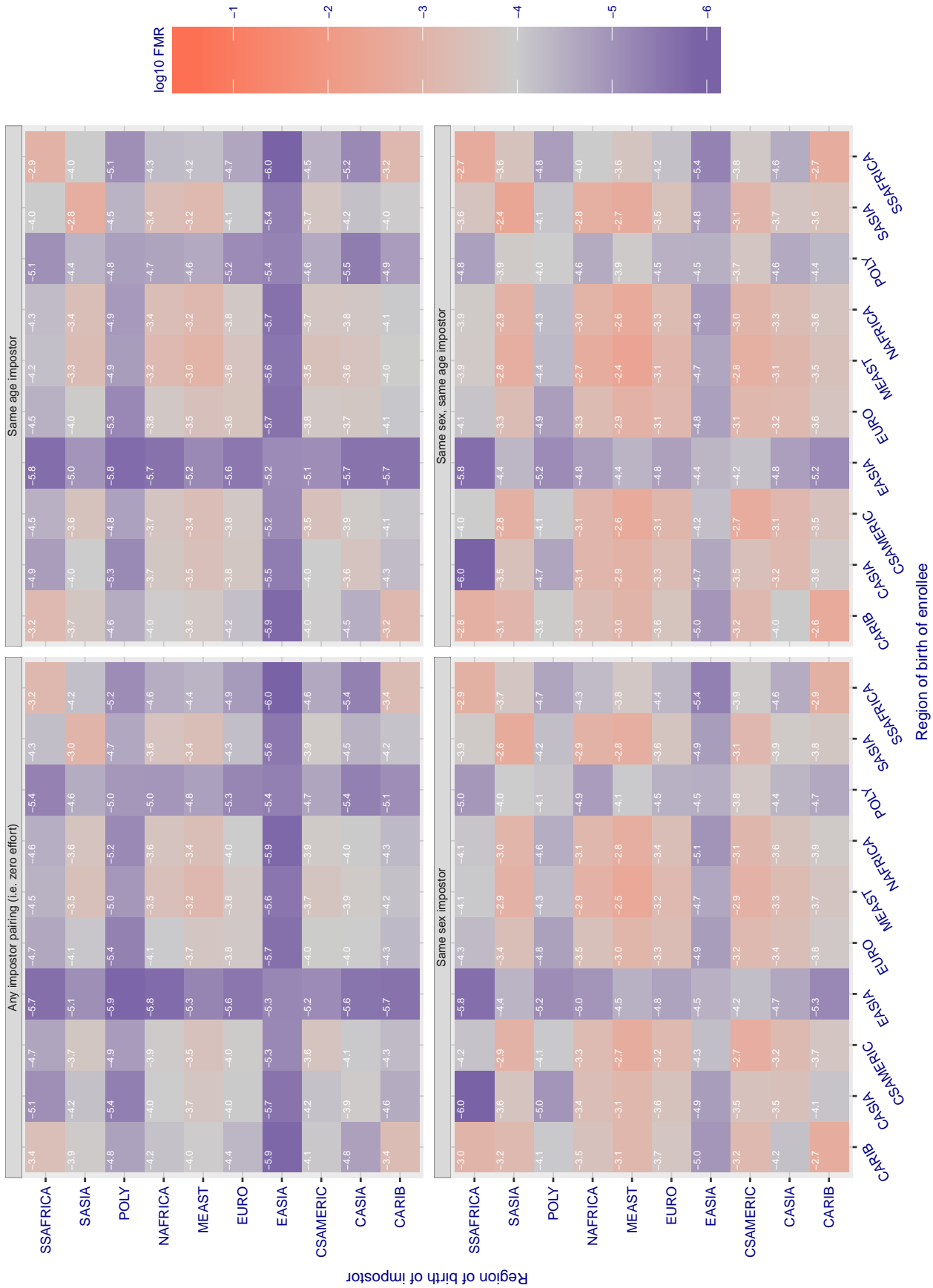


Figure 54: For algorithm pa-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.556$ for algorithm rankone_002, giving $FMR(T) = 0.0001$ globally.

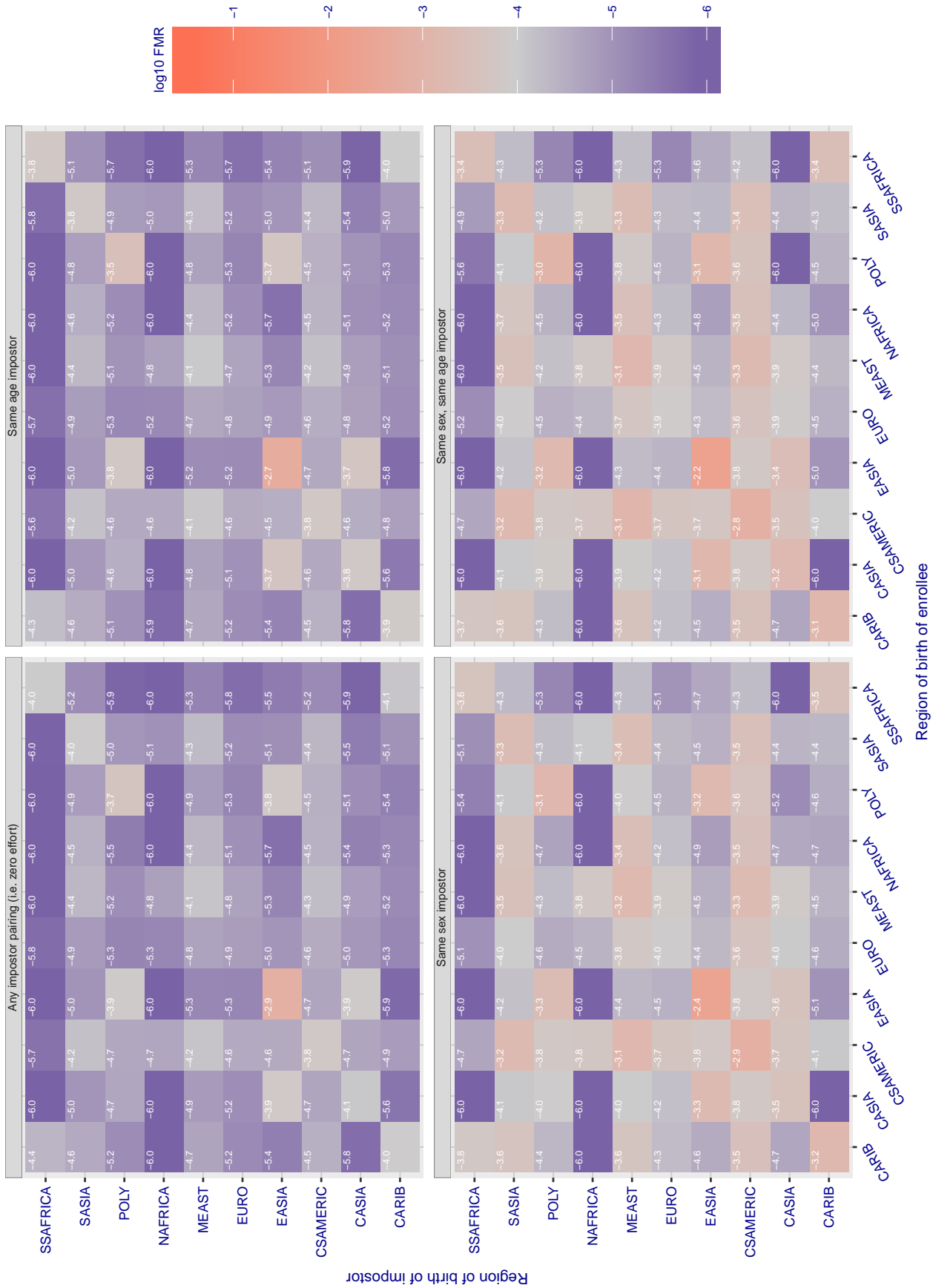


Figure 55: For algorithm rankone-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.710$ for algorithm rankone_003, giving $FMR(T) = 0.0001$ globally.

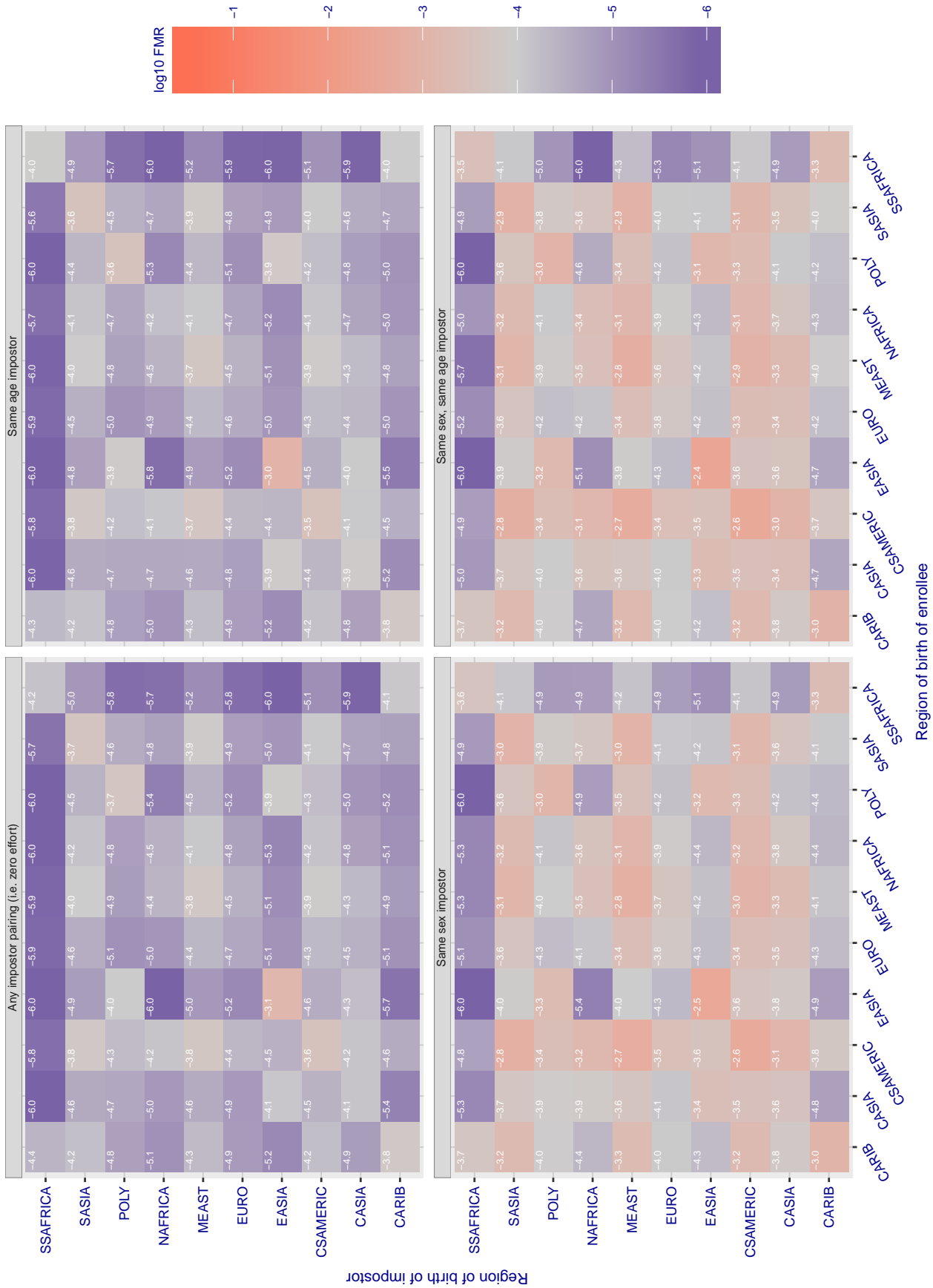


Figure 56: For algorithm rankone-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 80.766$ for algorithm samtech_000, giving $FMR(T) = 0.0001$ globally.

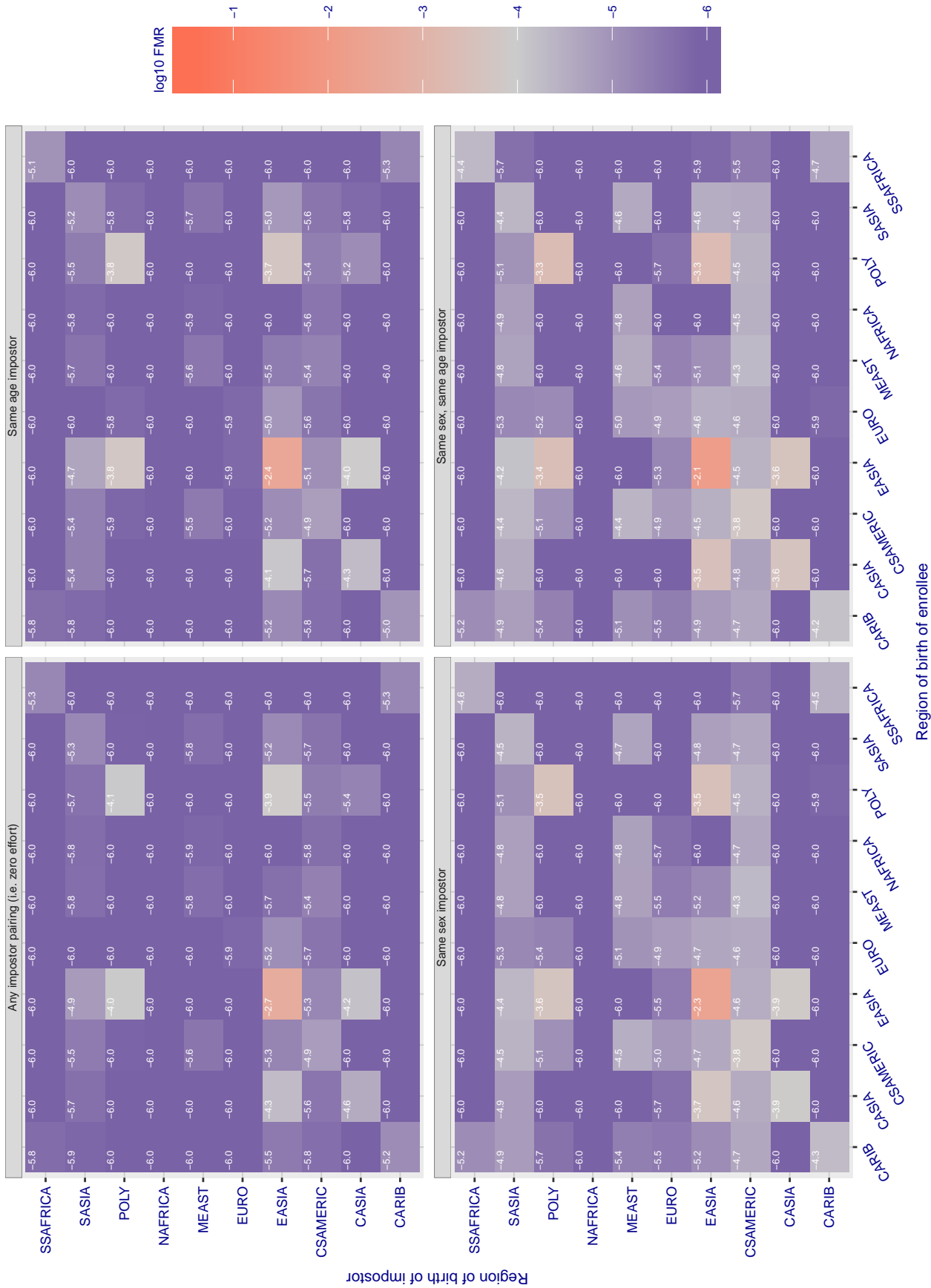


Figure 57: For algorithm samtech-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.970$ for algorithm shaman_000, giving $FMR(T) = 0.0001$ globally.

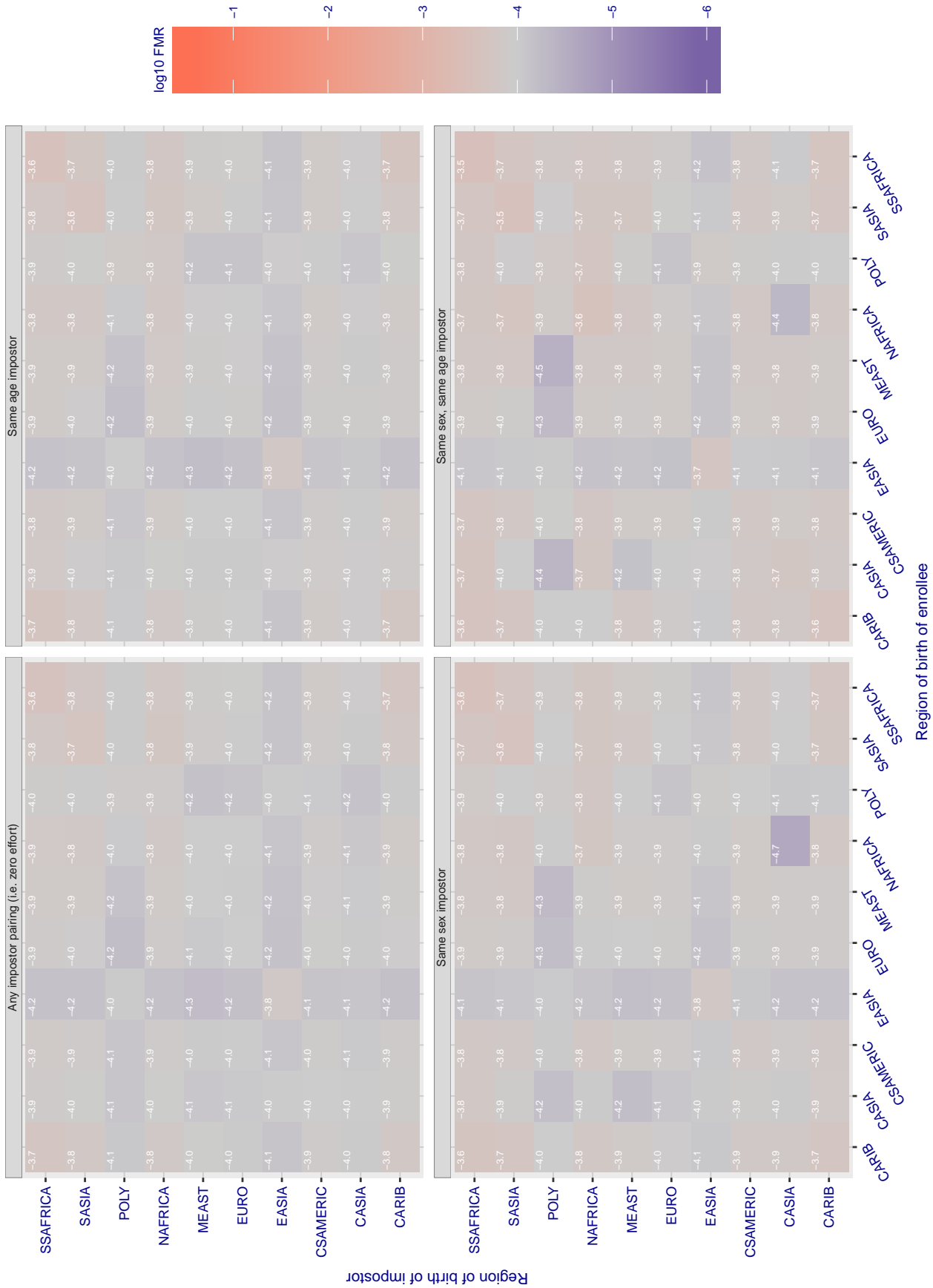


Figure 58: For algorithm shaman-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.725$ for algorithm shaman_001, giving $FMR(T) = 0.0001$ globally.

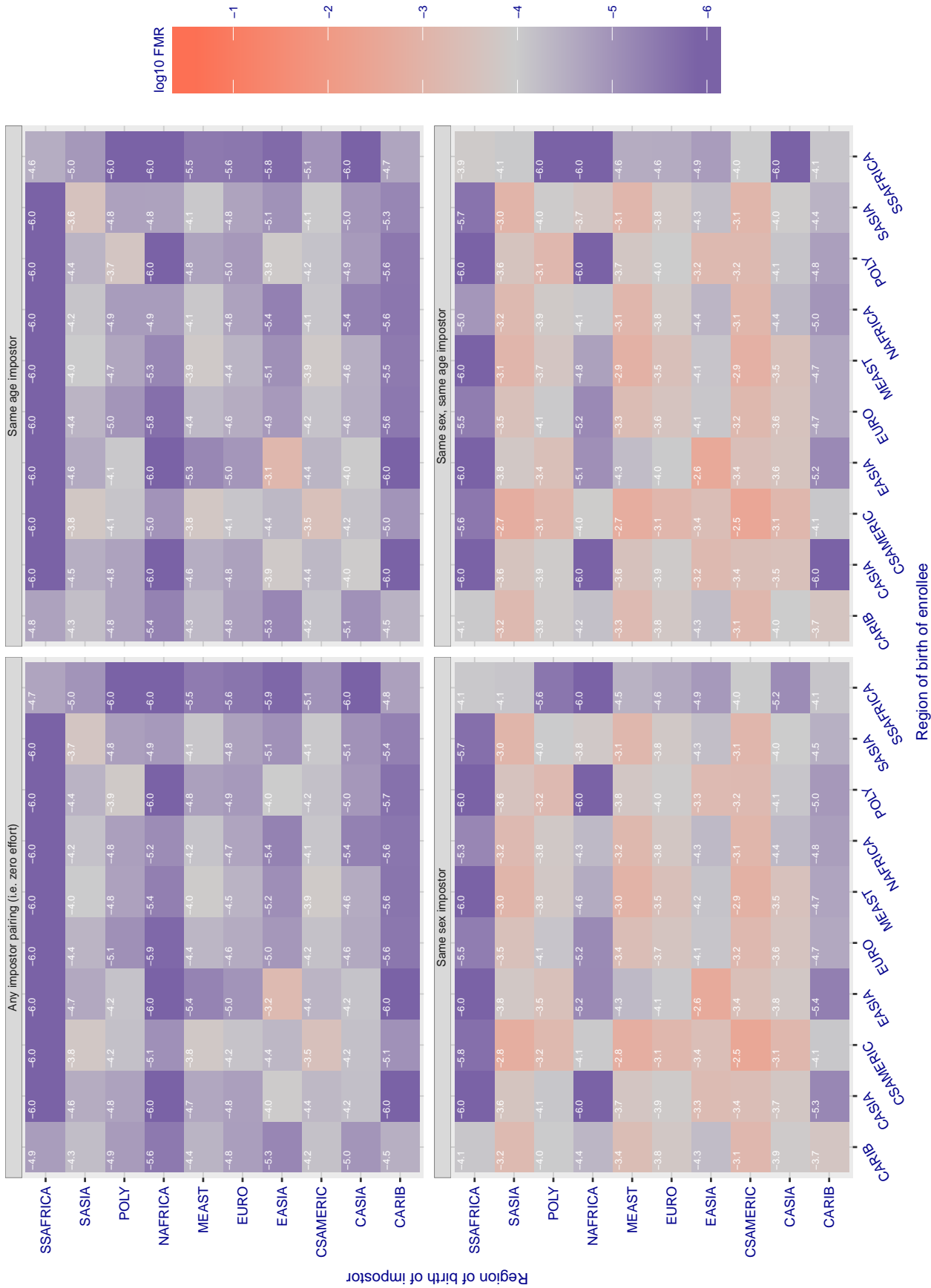


Figure 59: For algorithm shaman-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.929$ for algorithm `tevia_000`, giving $FMR(T) = 0.0001$ globally.

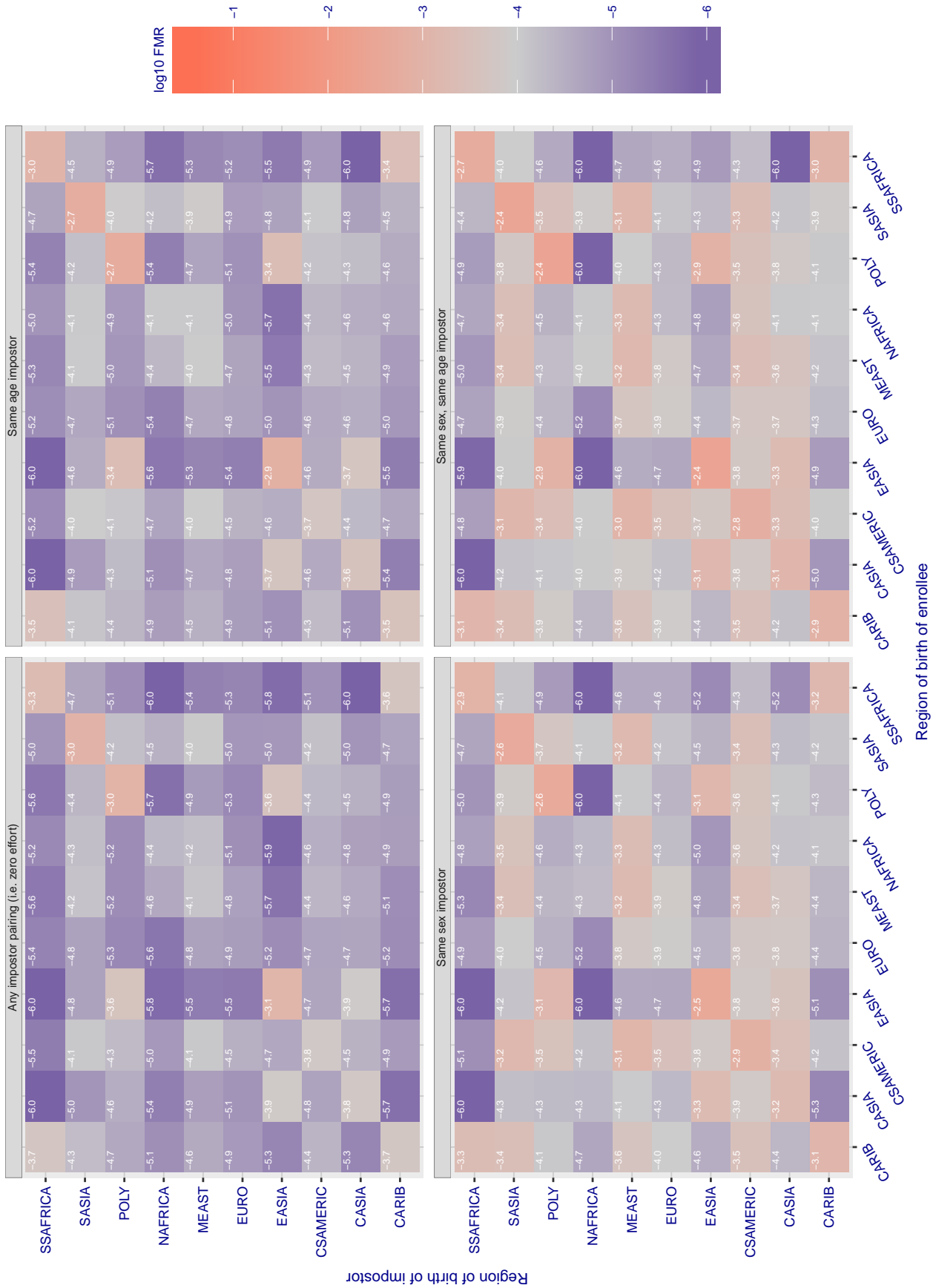


Figure 60: For algorithm `tevia_000` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 10.120$ for algorithm tongyitrans_001, giving $FMR(T) = 0.0001$ globally.

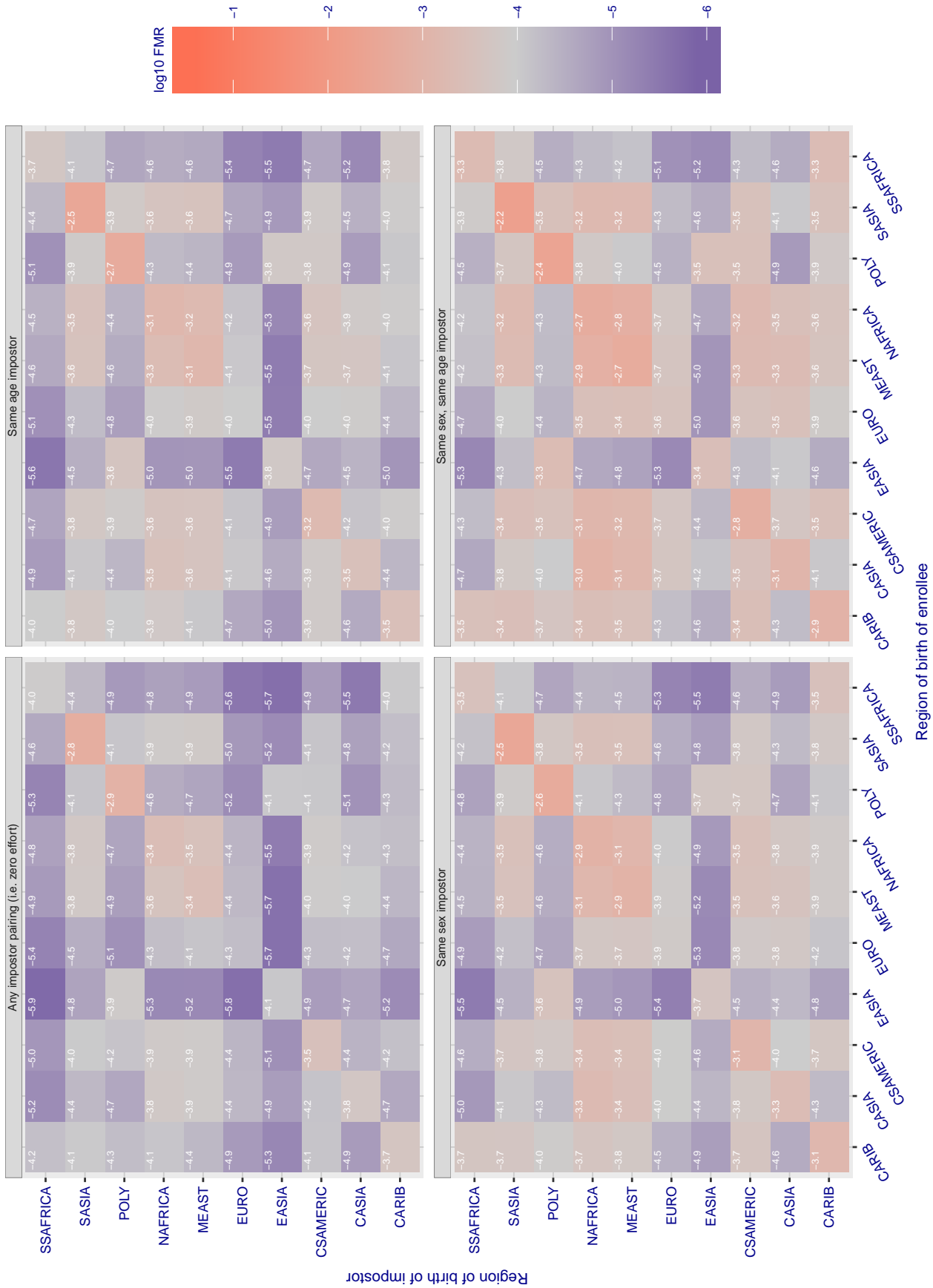


Figure 61: For algorithm tongyitrans-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 3.971$ for algorithm tongyitrans_002, giving $FMR(T) = 0.0001$ globally.

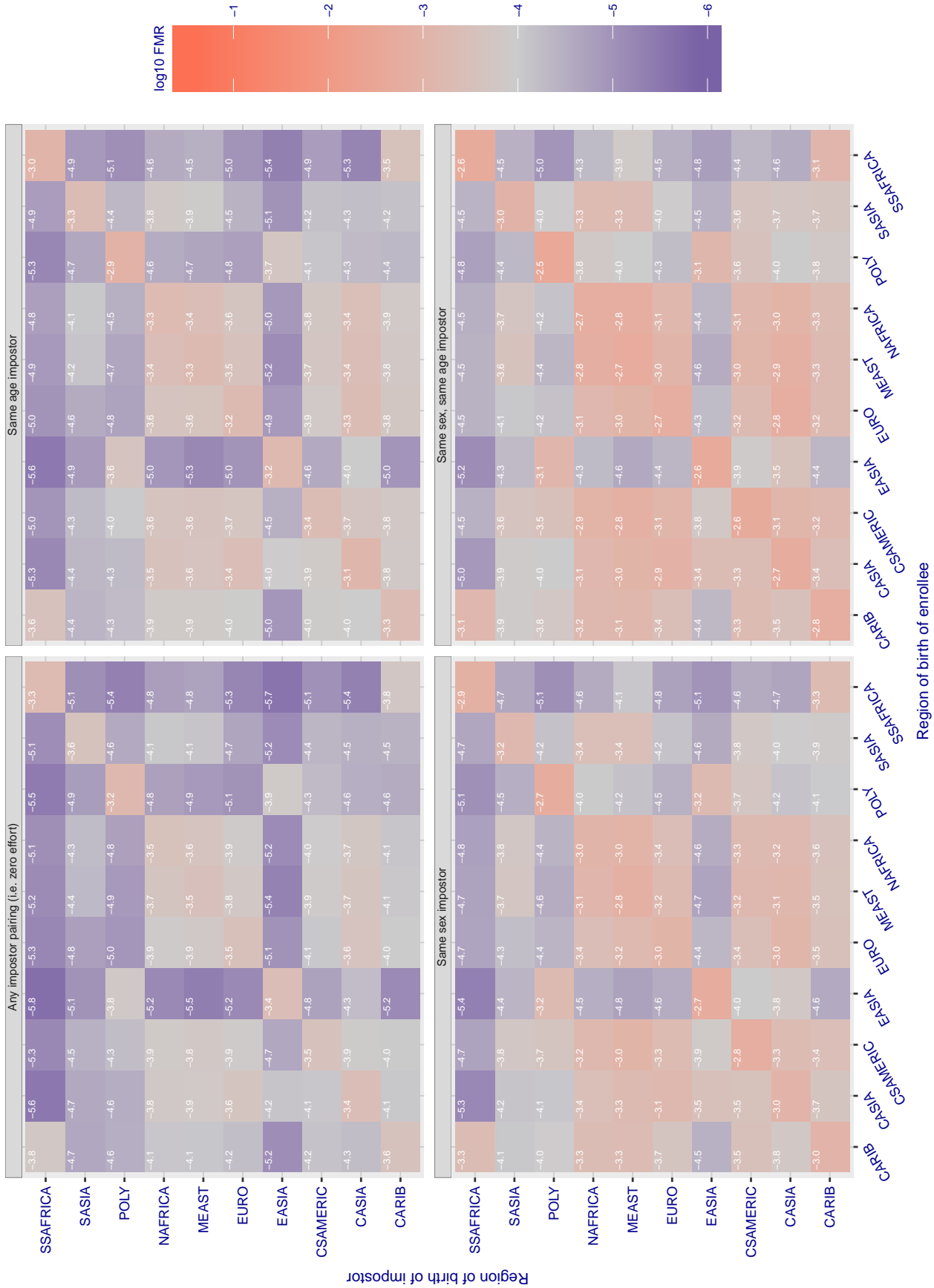


Figure 62: For algorithm tongyitrans-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.644$ for algorithm toshiba_000, giving $FMR(T) = 0.0001$ globally.

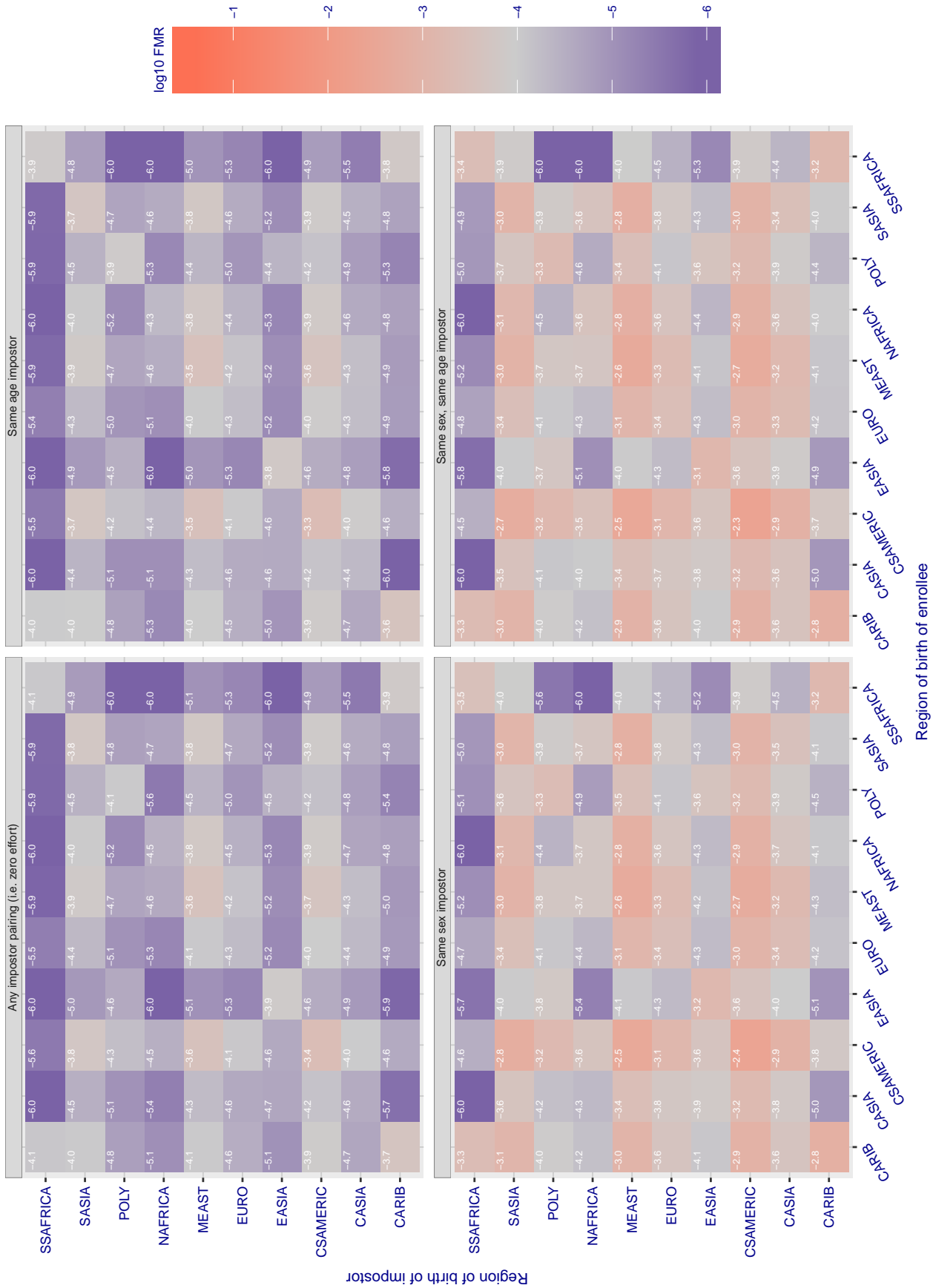


Figure 63: For algorithm toshiba-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.605$ for algorithm toshiba_001, giving $FMR(T) = 0.0001$ globally.

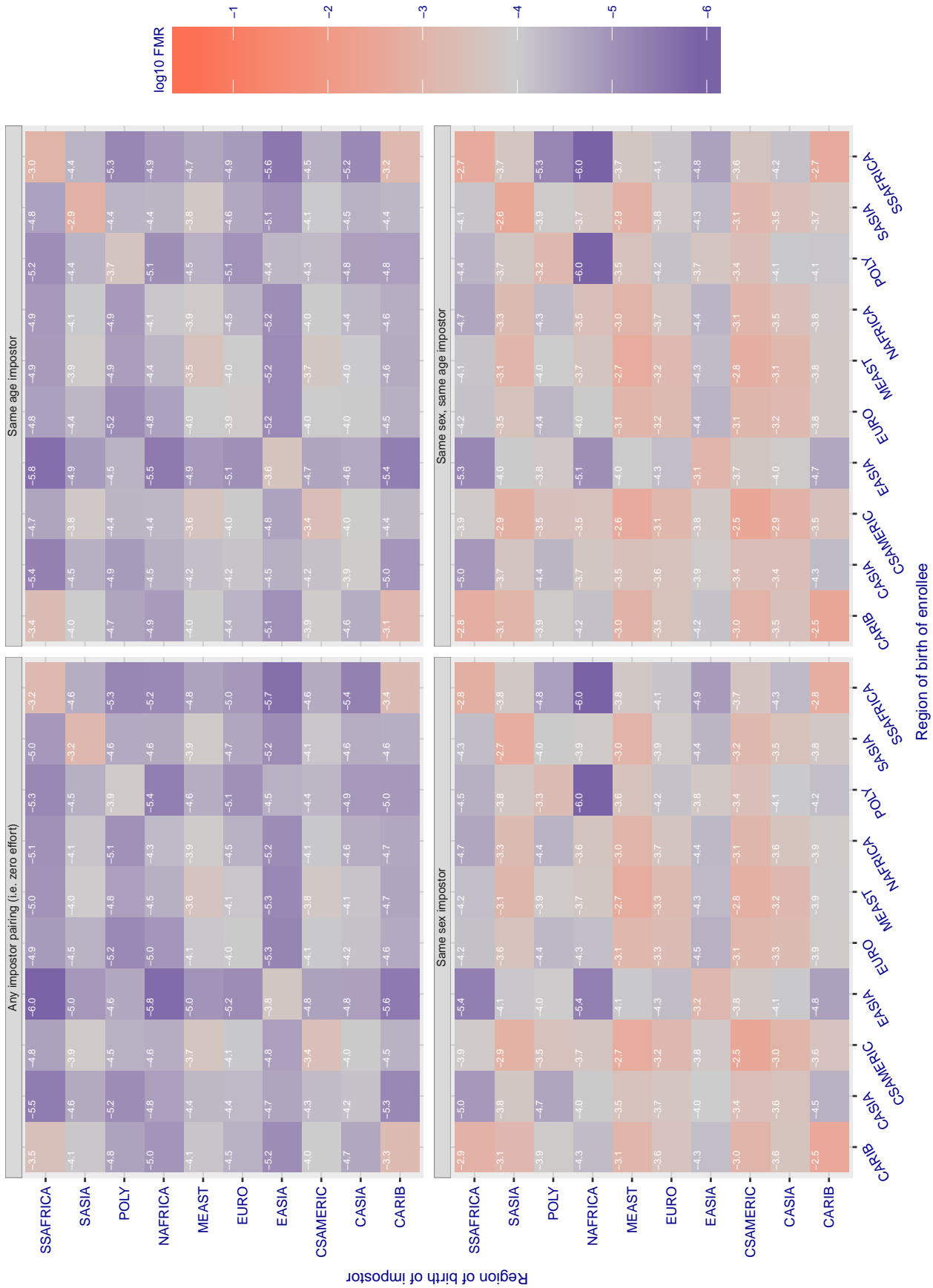


Figure 64: For algorithm toshiba-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.830$ for algorithm ultinous_000, giving $FMR(T) = 0.0001$ globally.

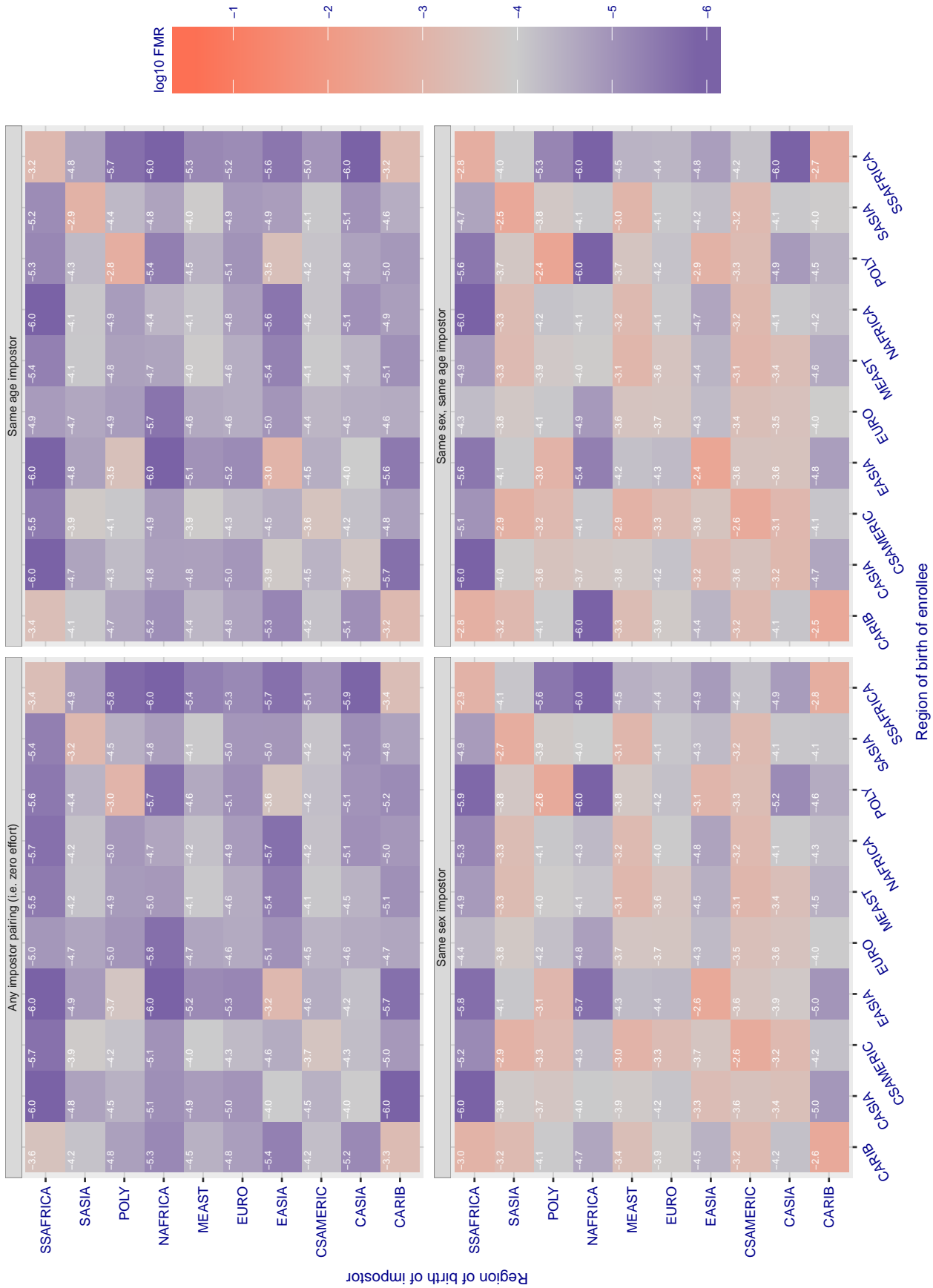


Figure 65: For algorithm ultinous-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.428$ for algorithm vcog_002, giving $FMR(T) = 0.0001$ globally.

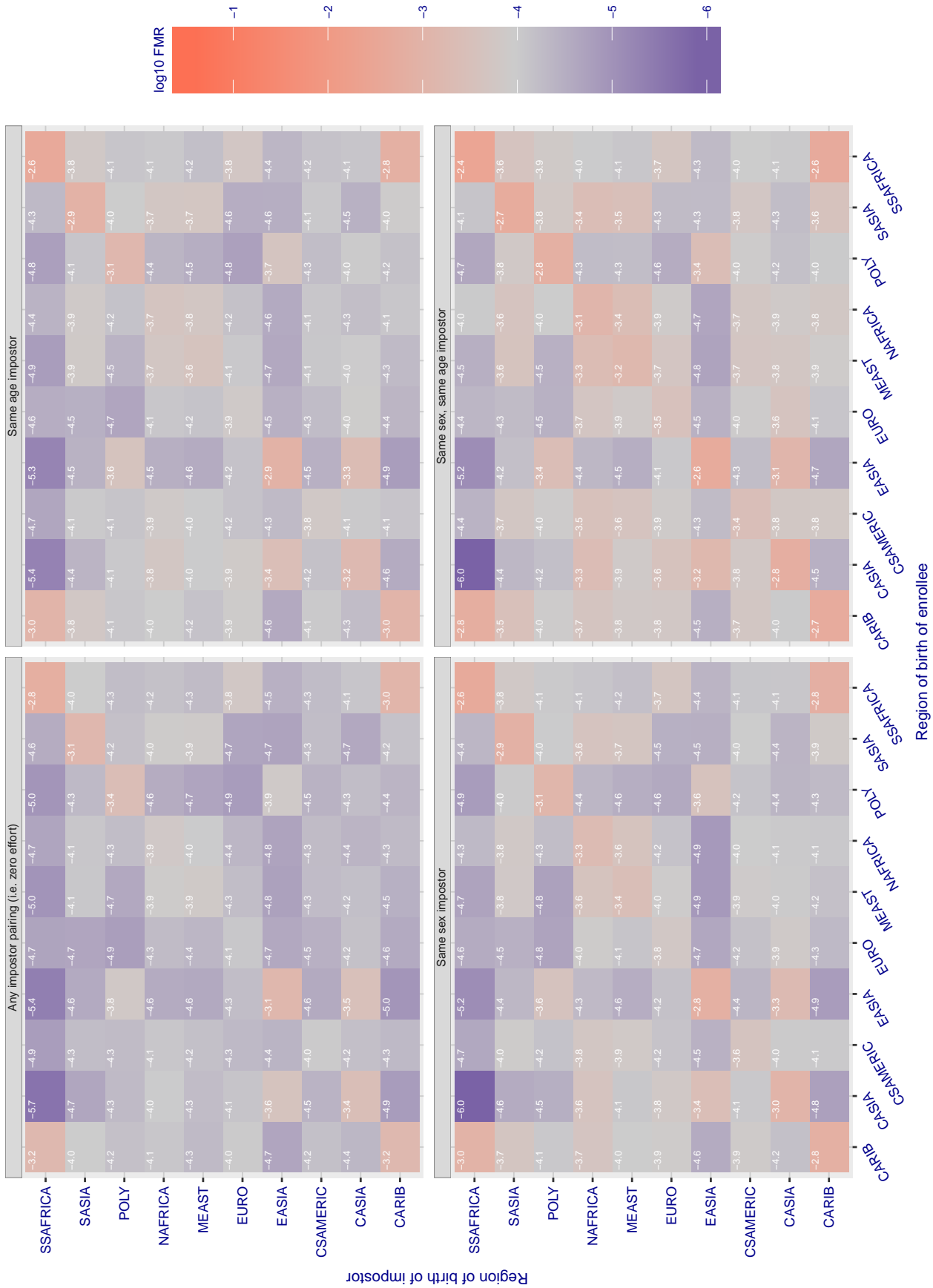


Figure 66: For algorithm vcog-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 4.315$ for algorithm vigilant solutions_002, giving $FMR(T) = 0.0001$ globally.

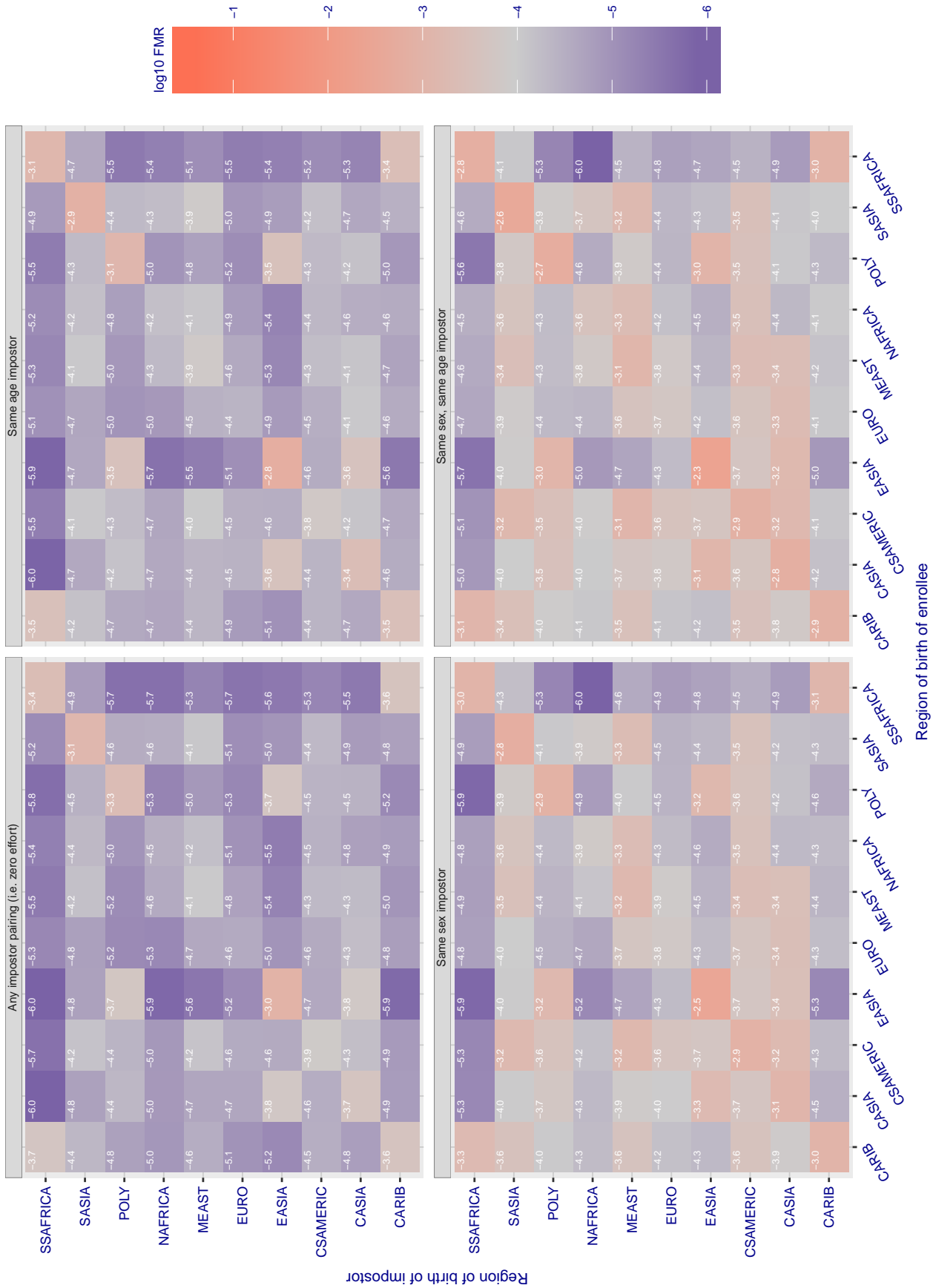


Figure 67: For algorithm vigilant solutions-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 3.308$ for algorithm vigilantolutions_003, giving $FMR(T) = 0.0001$ globally.

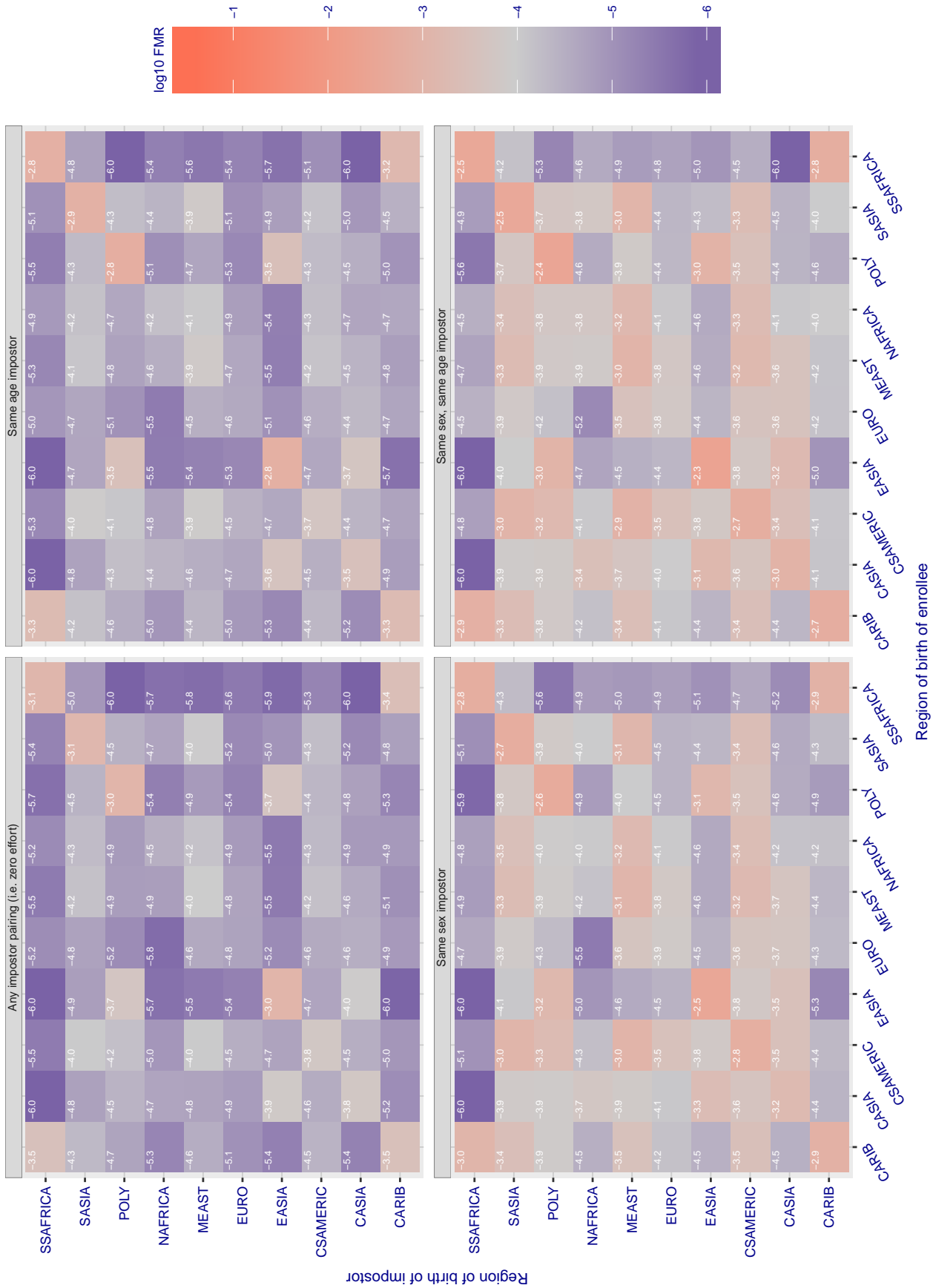


Figure 68: For algorithm vigilantolutions-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.080$ for algorithm visionlabs_001, giving $FMR(T) = 0.0001$ globally.

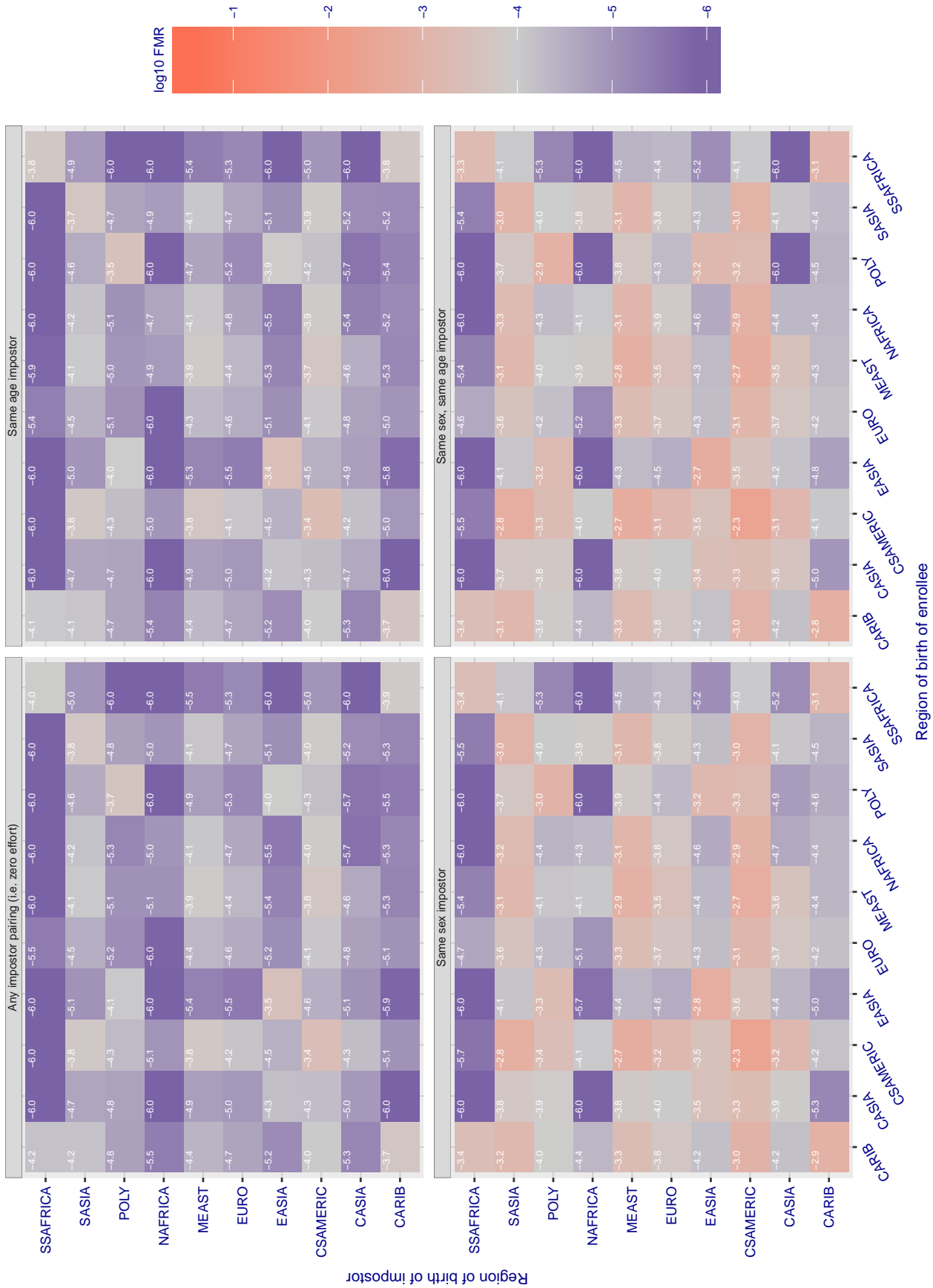


Figure 69: For algorithm visionlabs-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.794$ for algorithm visionlabs_002, giving $FMR(T) = 0.0001$ globally.

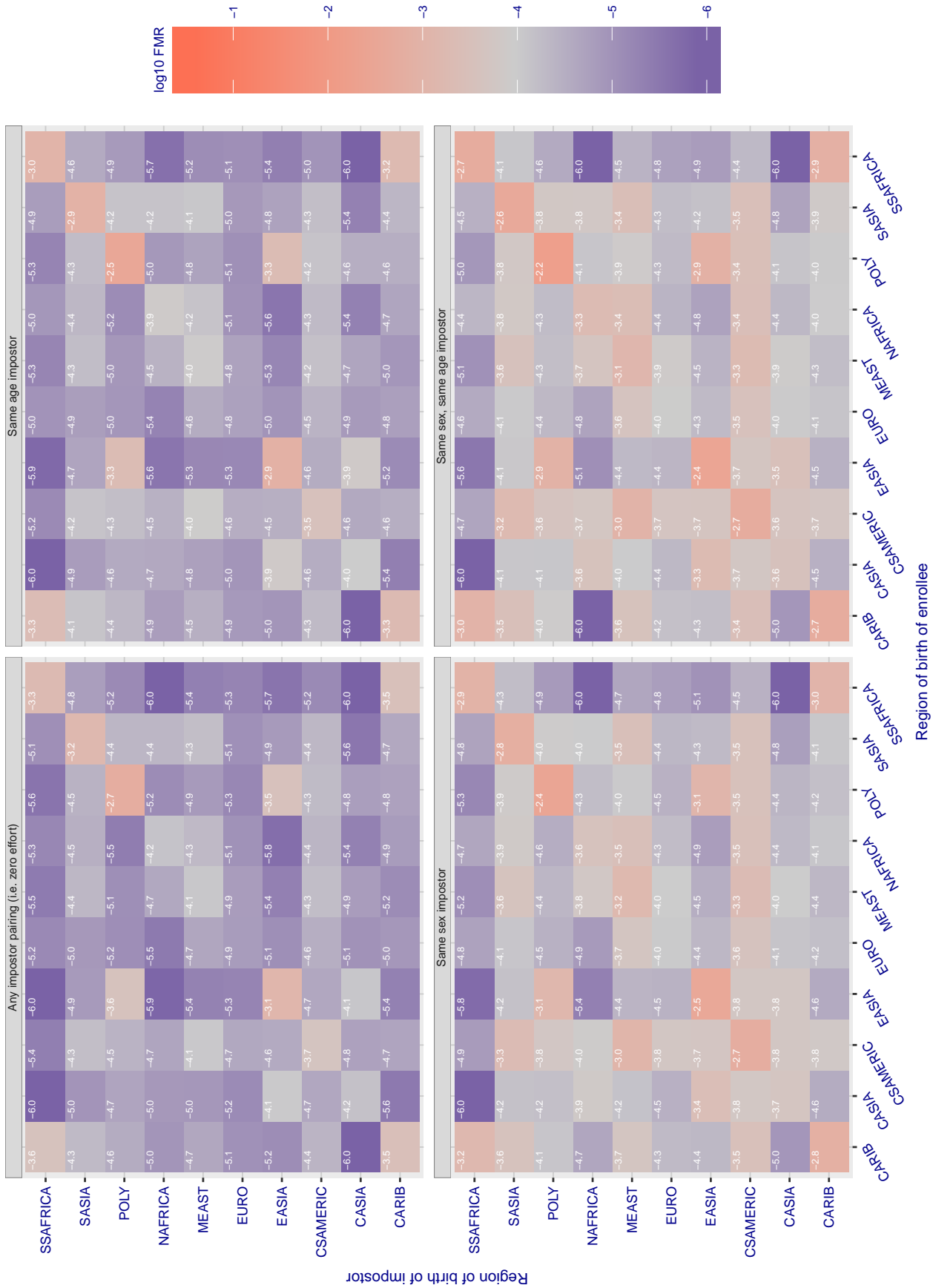


Figure 70: For algorithm visionlabs-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 0.867$ for algorithm vocord_002, giving $FMR(T) = 0.0001$ globally.

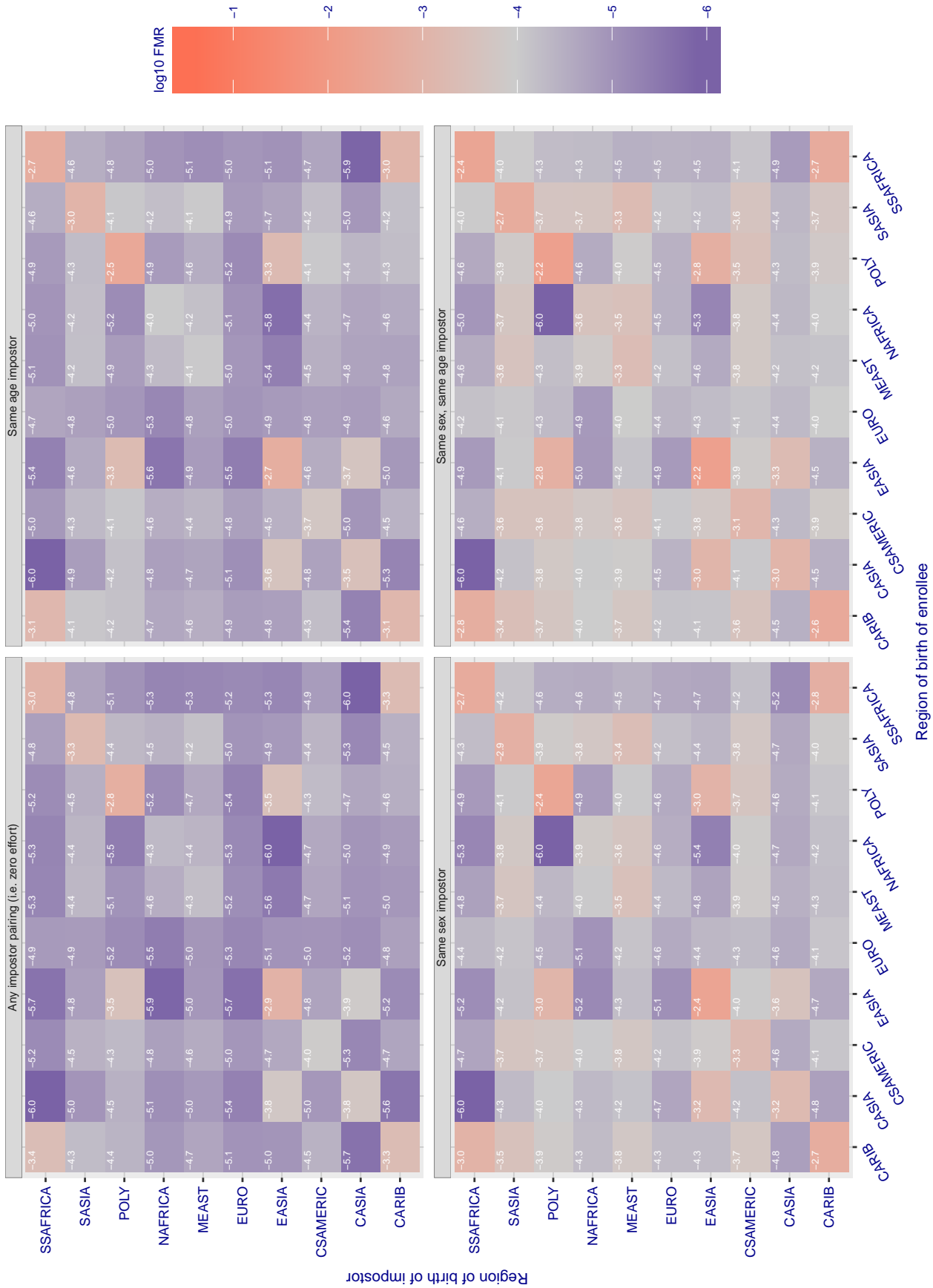


Figure 71: For algorithm vocord-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 6.196$ for algorithm yisheng_000, giving $FMR(T) = 0.0001$ globally.

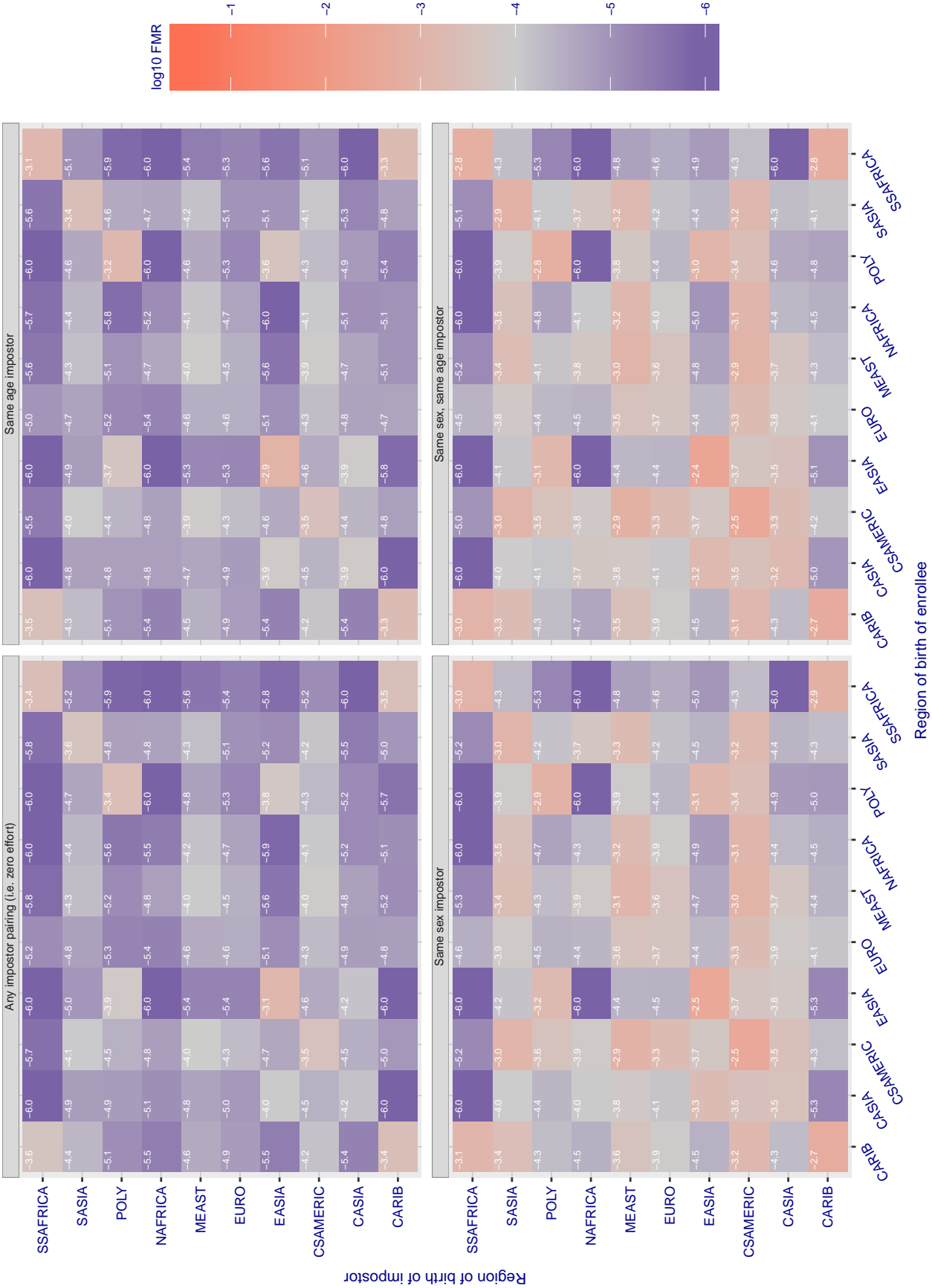


Figure 72: For algorithm yisheng-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 6.278$ for algorithm yisheng_001, giving $FMR(T) = 0.0001$ globally.

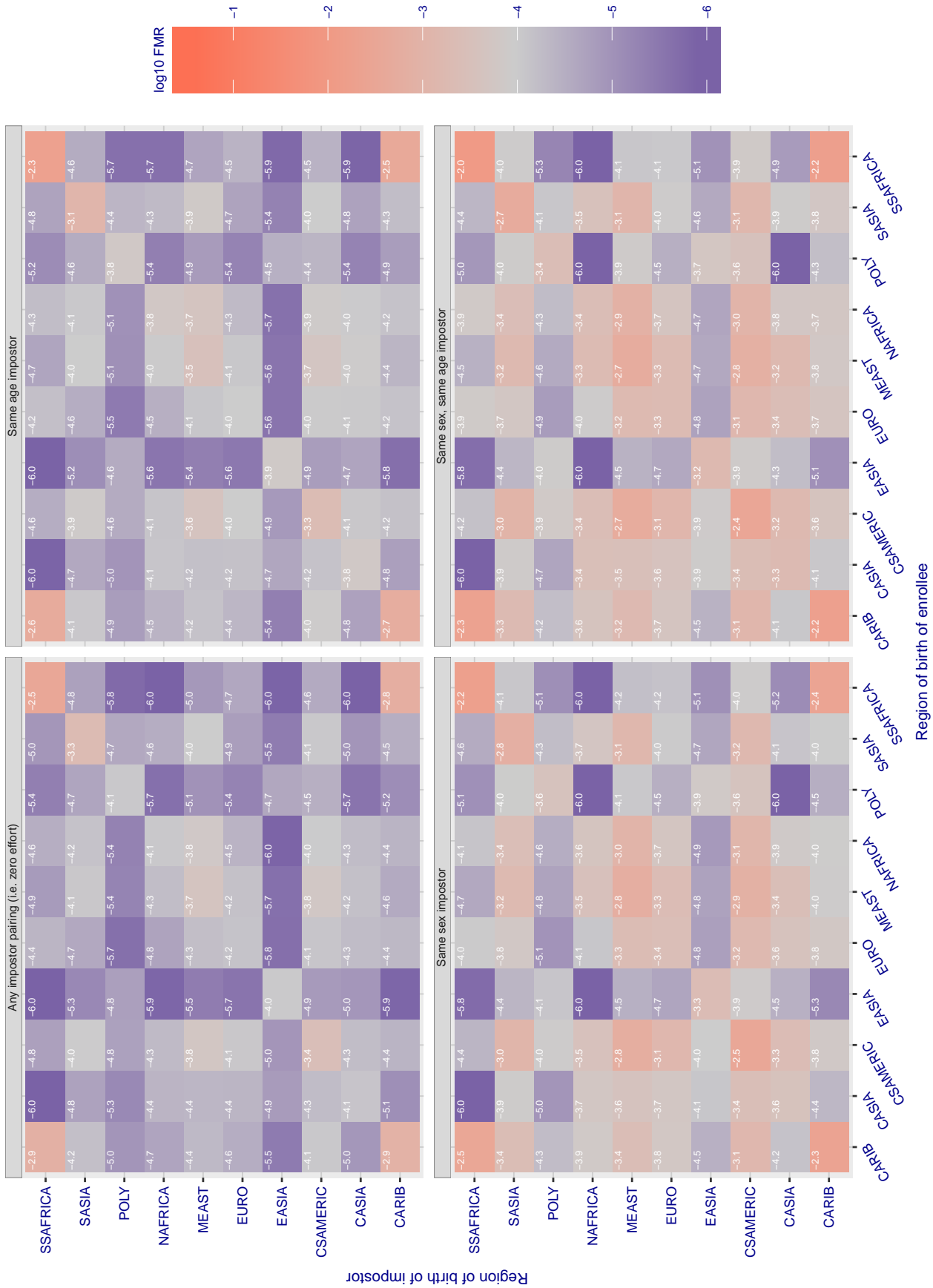


Figure 73: For algorithm yisheng-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross region FMR at threshold $T = 10.098$ for algorithm yitu_000, giving $FMR(T) = 0.0001$ globally.

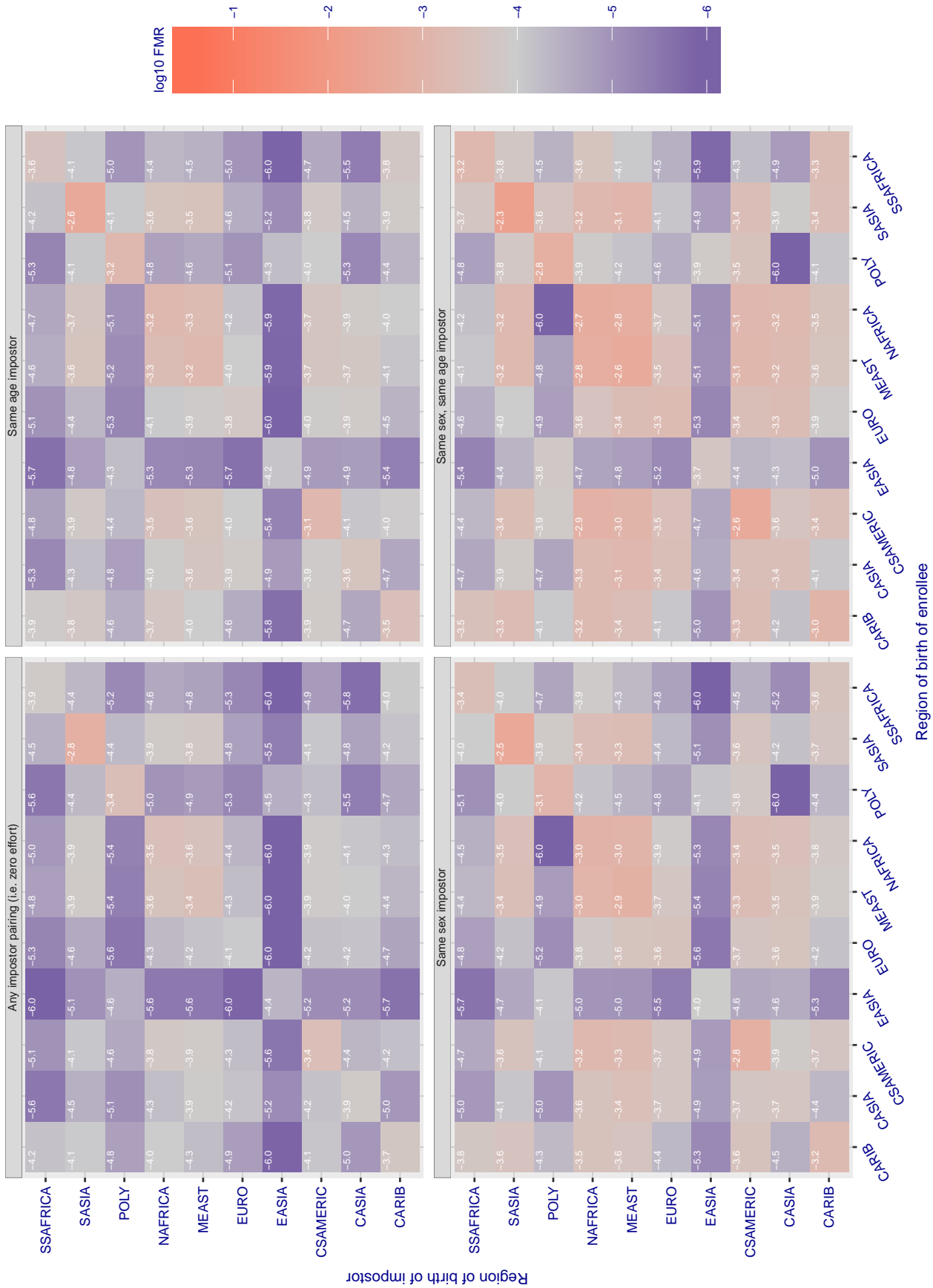
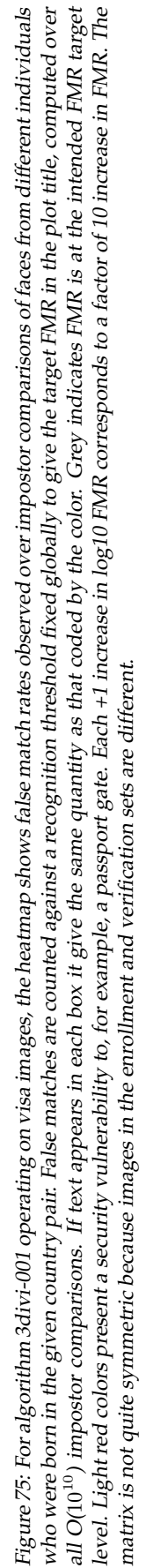


Figure 74: For algorithm yitu-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given region pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold $T = 2.675$ for algorithm 3divi_002, giving $FMR(T) = 0.001$ globally.

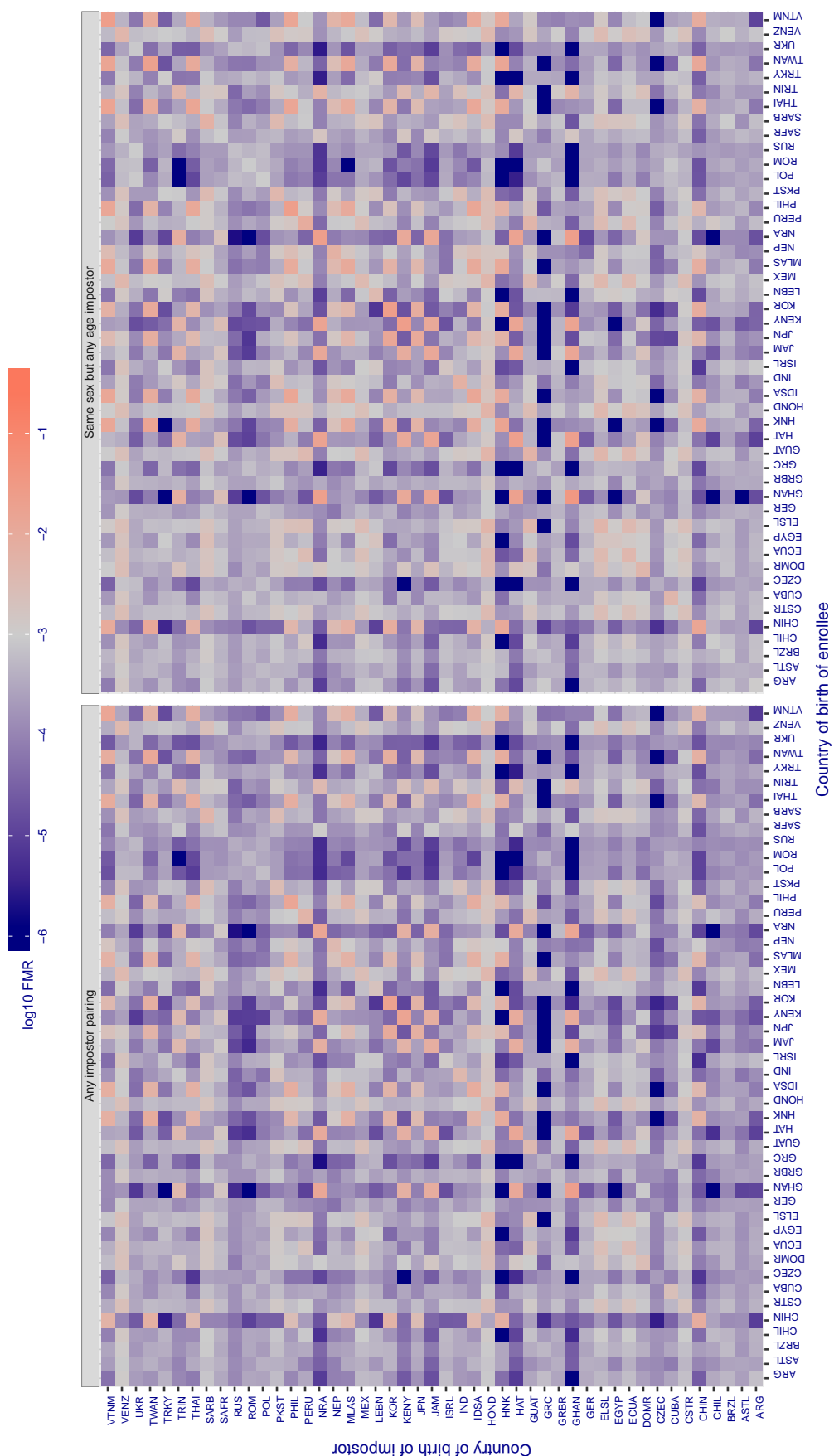


Figure 76: For algorithm 3divi-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each $+1$ increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

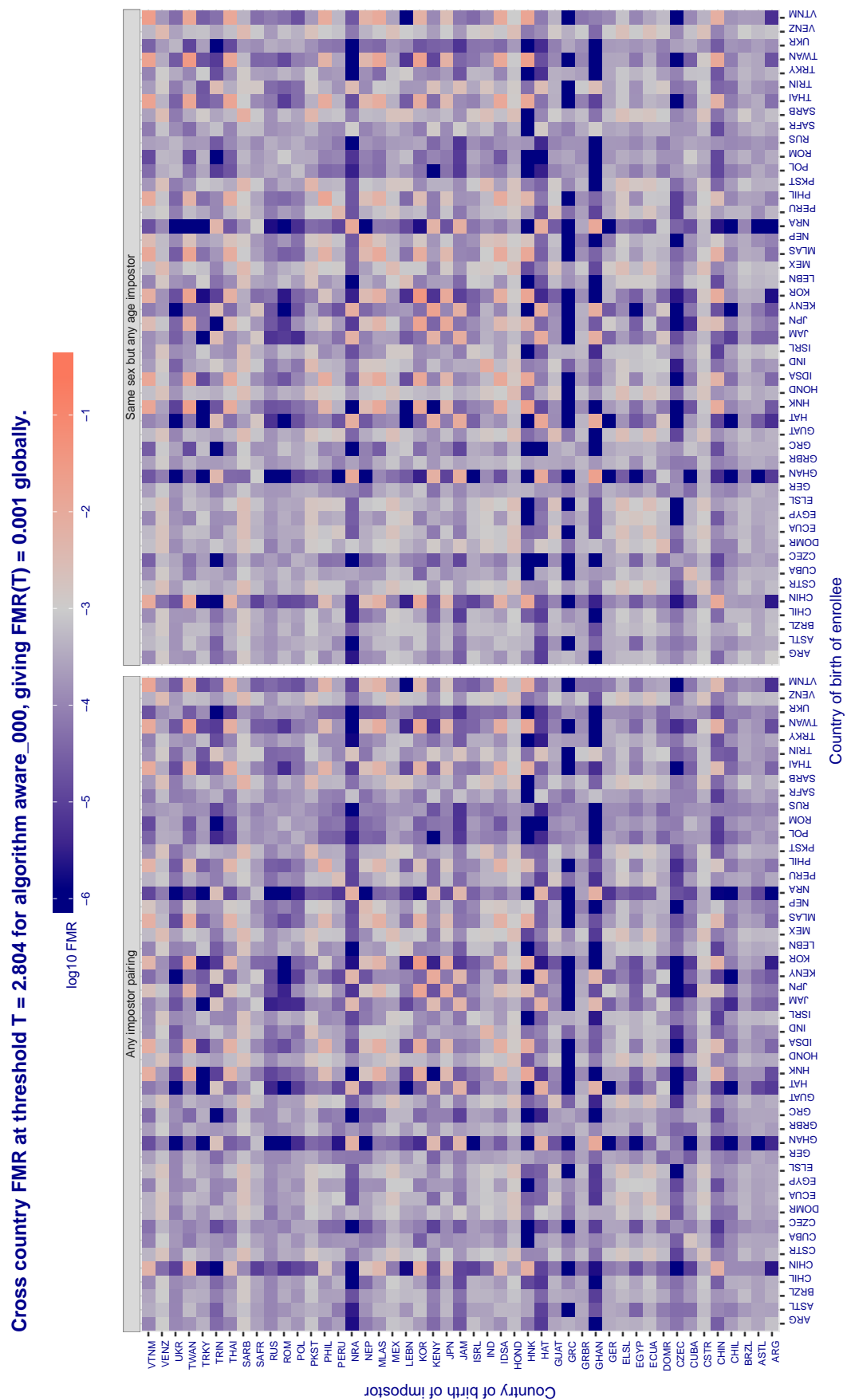


Figure 77: For algorithm aware-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 2.804$ for algorithm aware_001, giving $FMR(T) = 0.001$ globally.

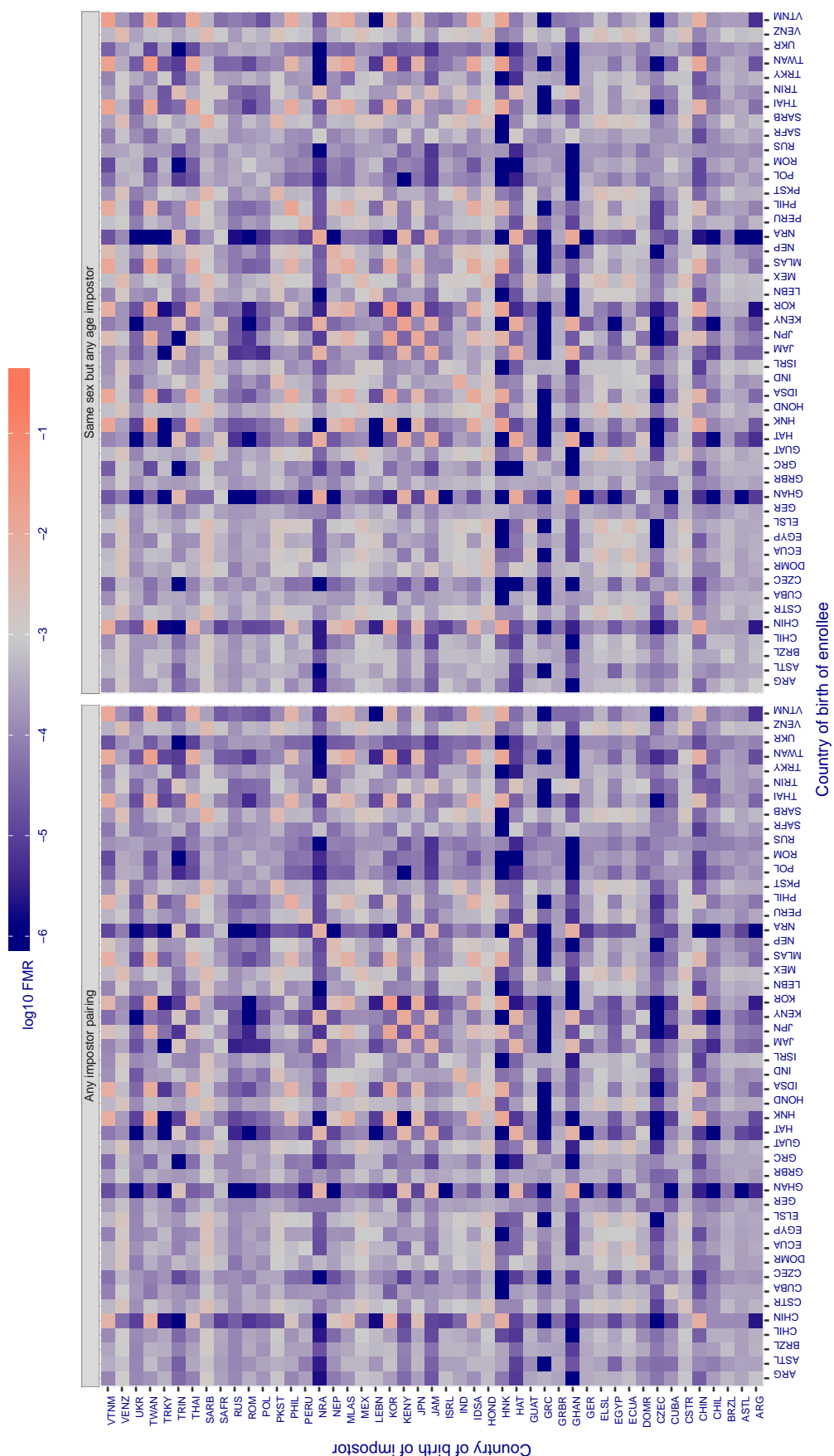


Figure 78: For algorithm aware-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 0.800$ for algorithm ayonix_000, giving $FMR(T) = 0.001$ globally.

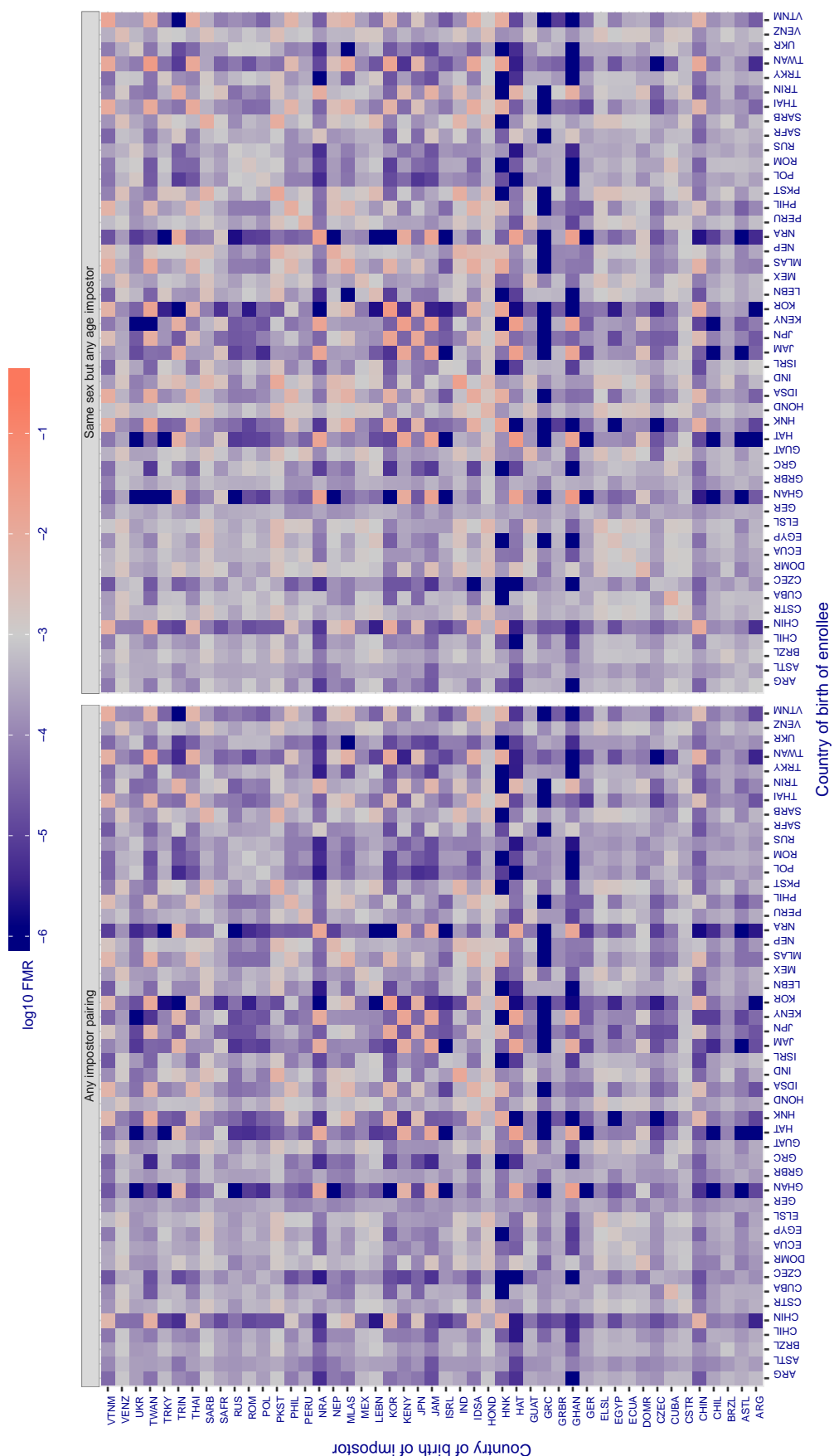


Figure 79: For algorithm ayonix-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 0.577$ for algorithm camvi_001, giving $FMR(T) = 0.001$ globally.

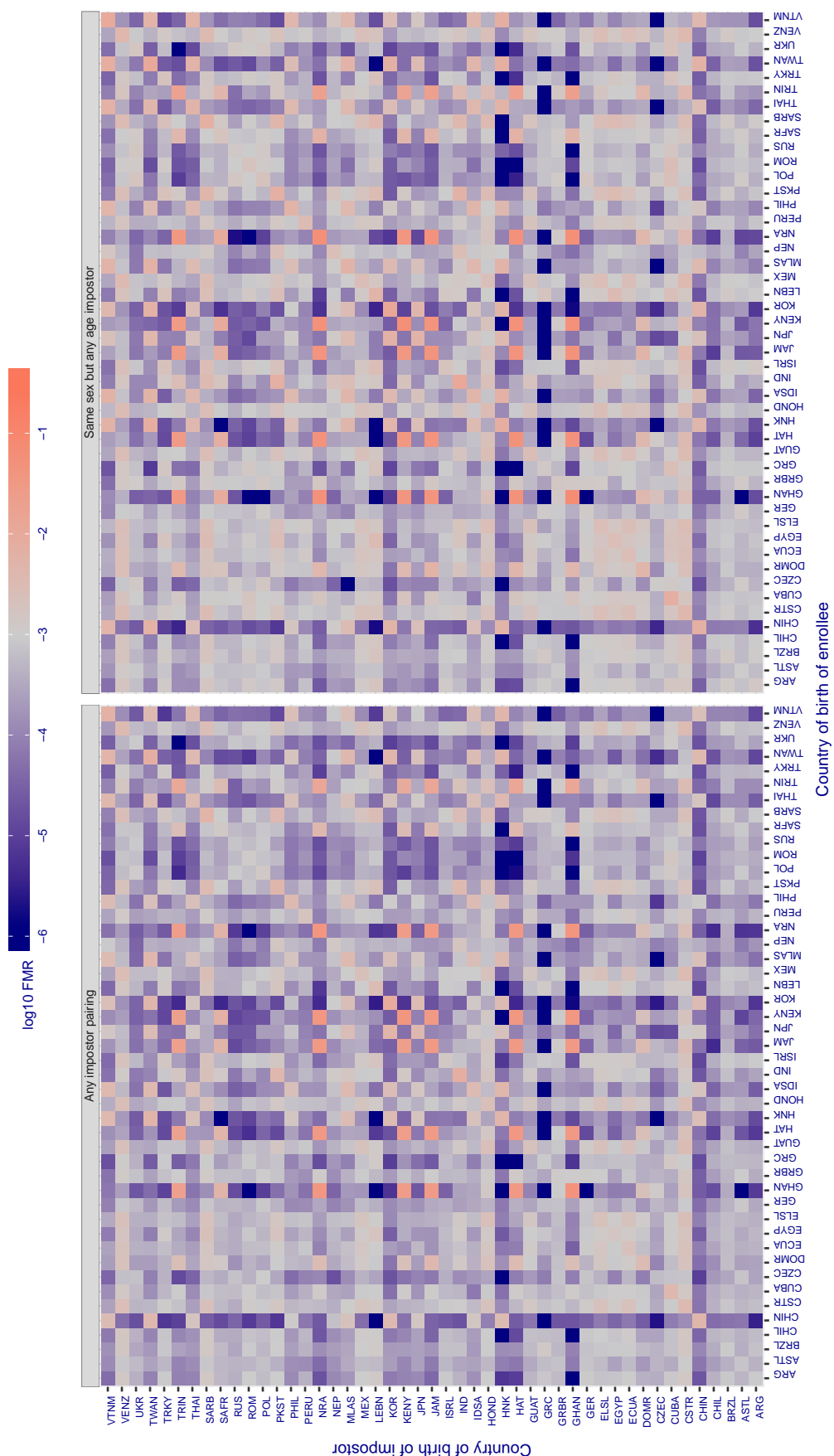


Figure 80: For algorithm camvi-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 3230.000$ for algorithm cogent_000, giving $FMR(T) = 0.001$ globally.

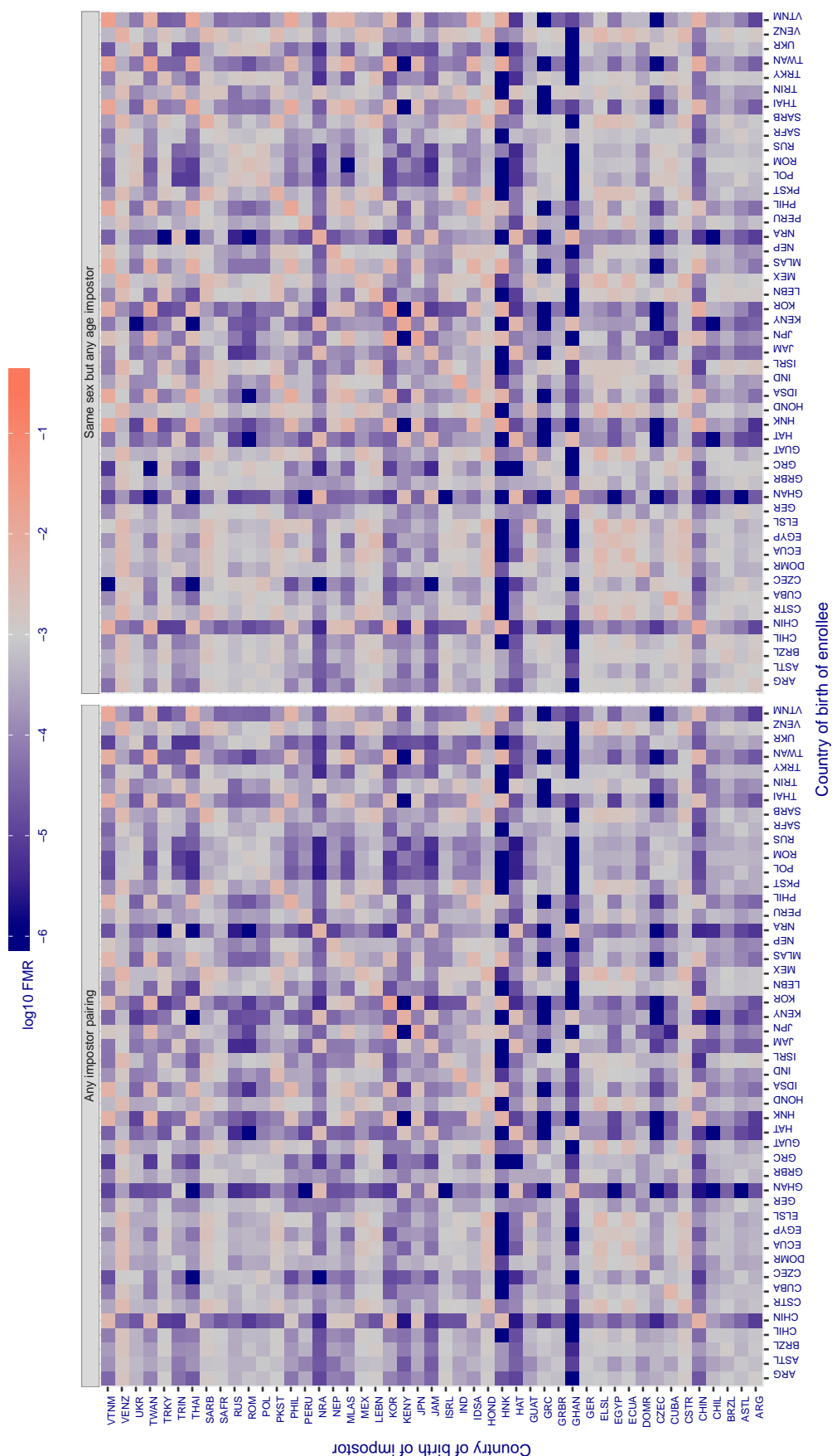


Figure 81: For algorithm cogent-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log₁₀ FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 0.702$ for algorithm cyberextruder_001, giving $FMR(T) = 0.001$ globally.

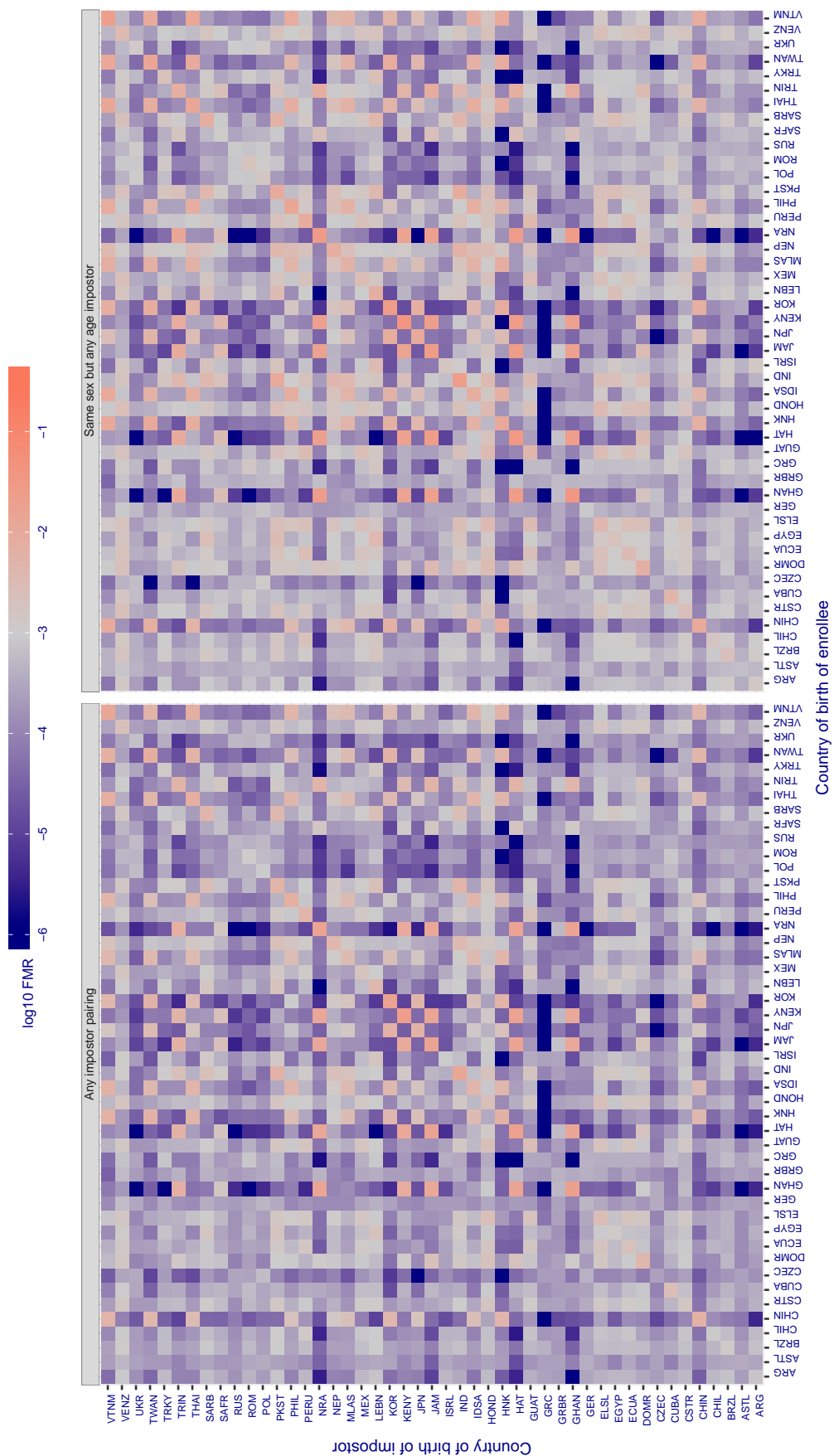
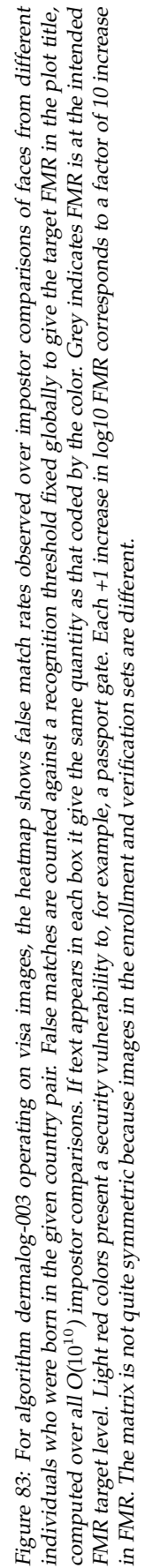


Figure 82: For algorithm cyberextruder-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold $T = 78.891$ for algorithm dermalog_004, giving $FMR(T) = 0.001$ globally.

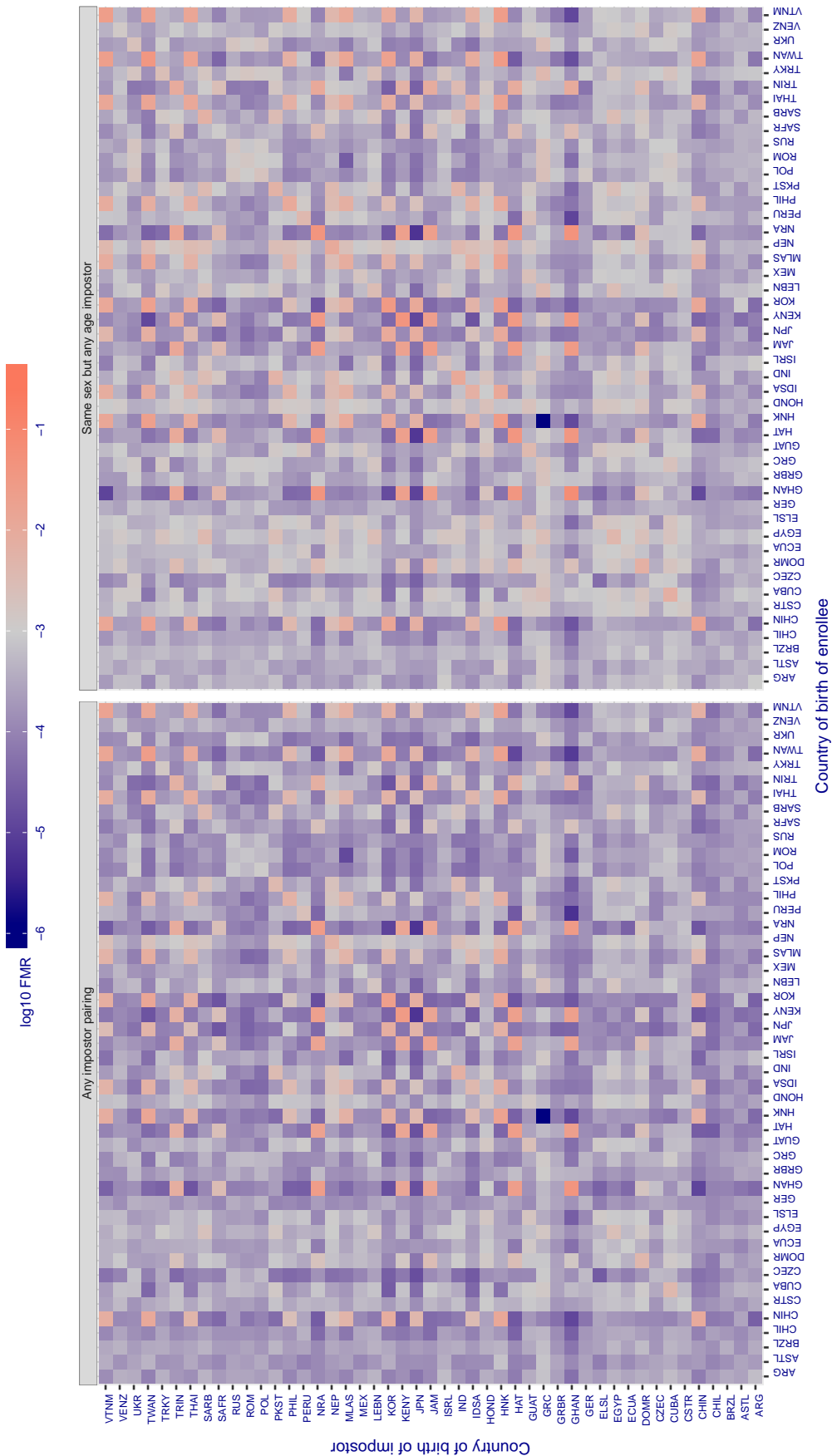


Figure 84: For algorithm dermalog-004 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 0.554$ for algorithm digitalbarriers_000, giving $FMR(T) = 0.001$ globally.

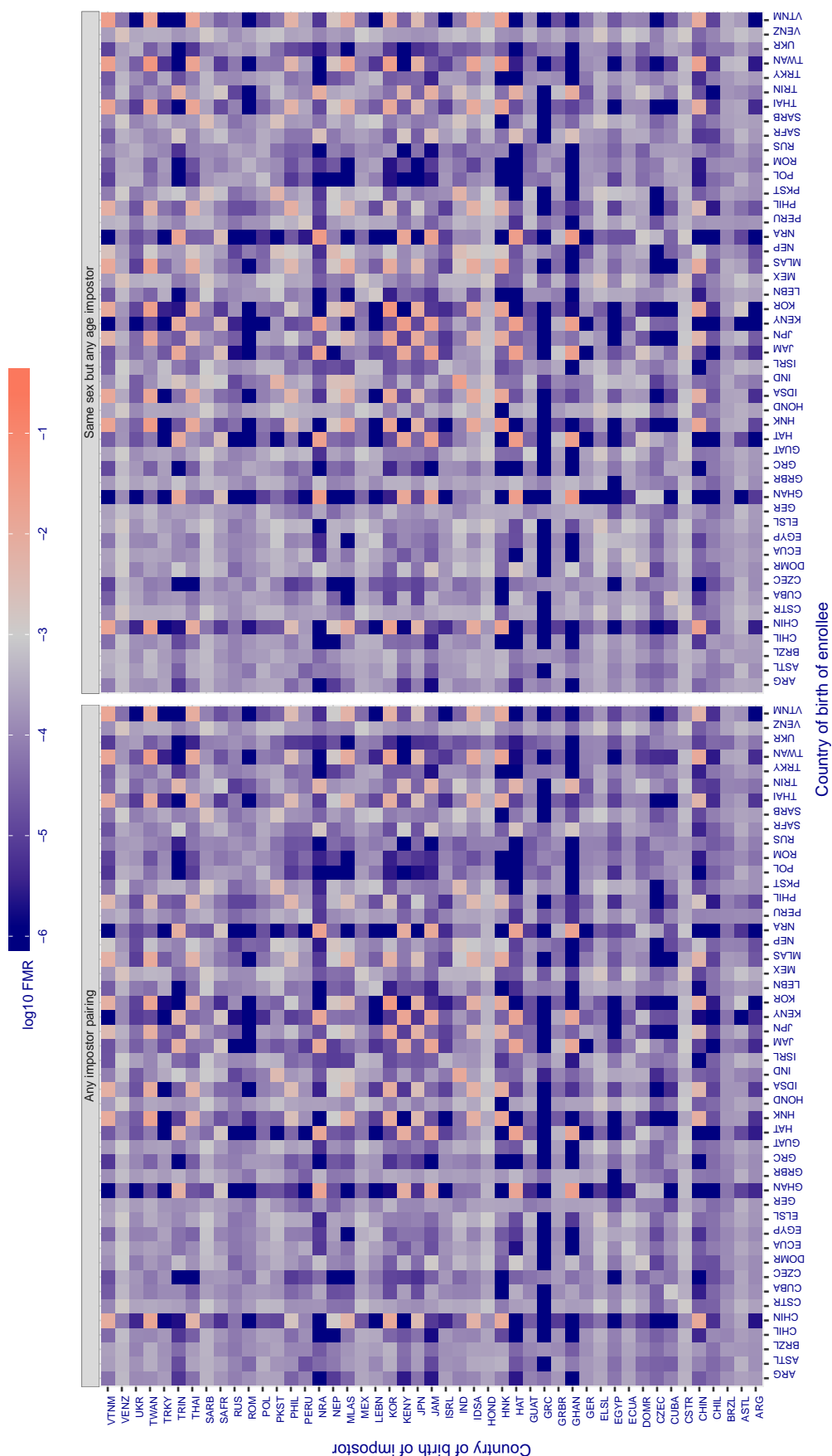
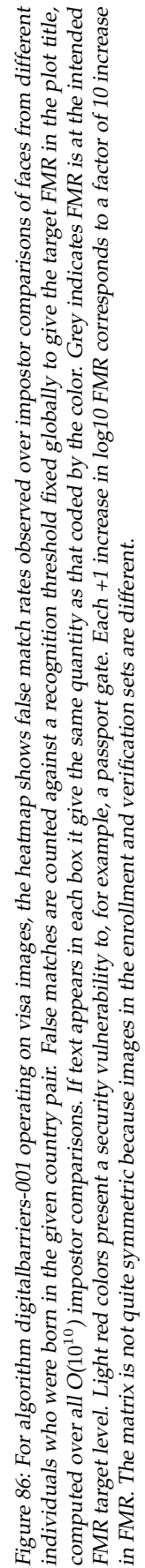


Figure 85: For algorithm digitalbarriers-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold $T = 0.575$ for algorithm fdu_000 , giving $\text{FMR}(T) = 0.001$ globally.

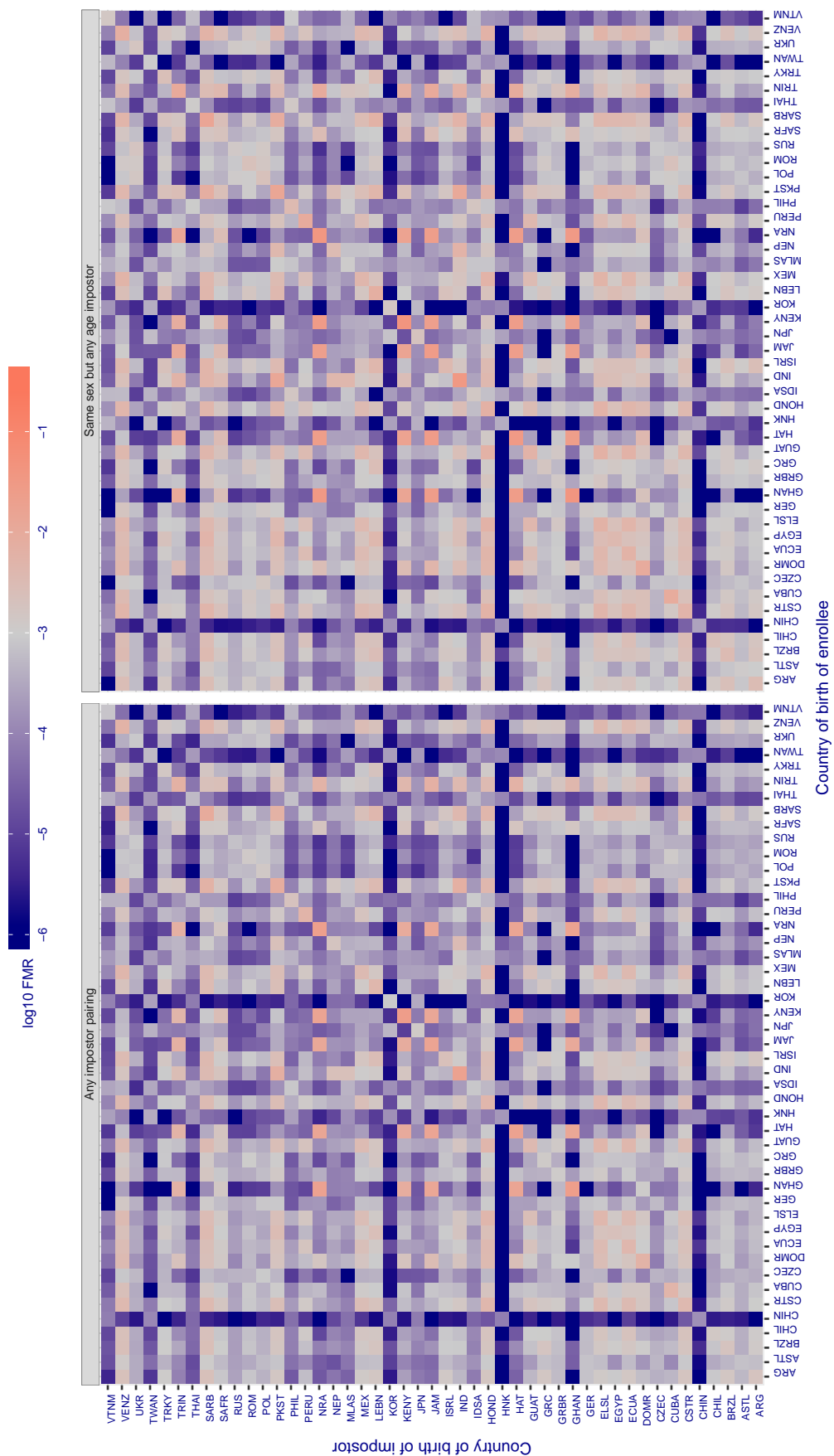


Figure 87: For algorithm fdu-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each $+1$ increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

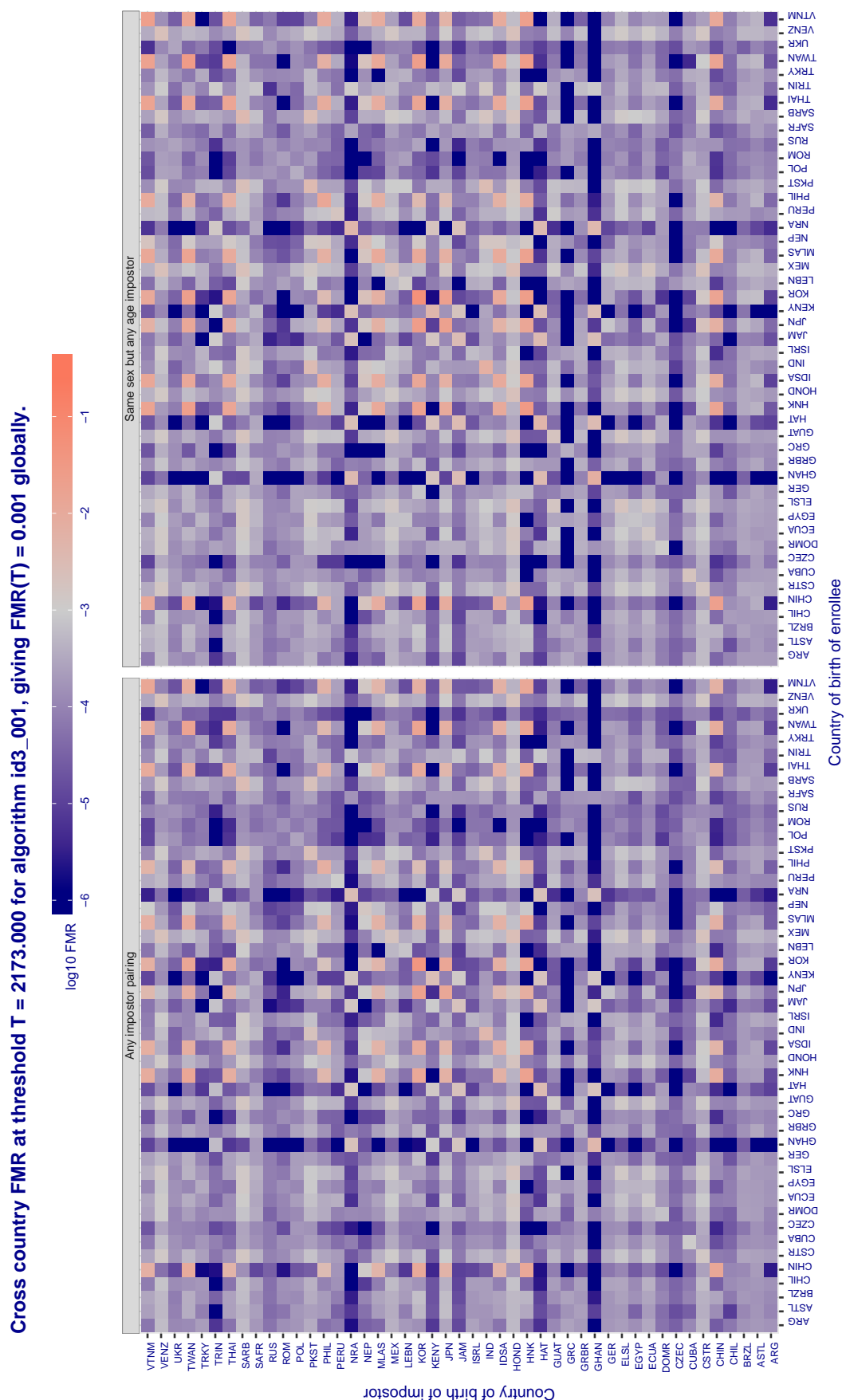


Figure 88: For algorithm id3-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log₁₀ FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 2204.000$ for algorithm id3_002, giving $FMR(T) = 0.001$ globally.

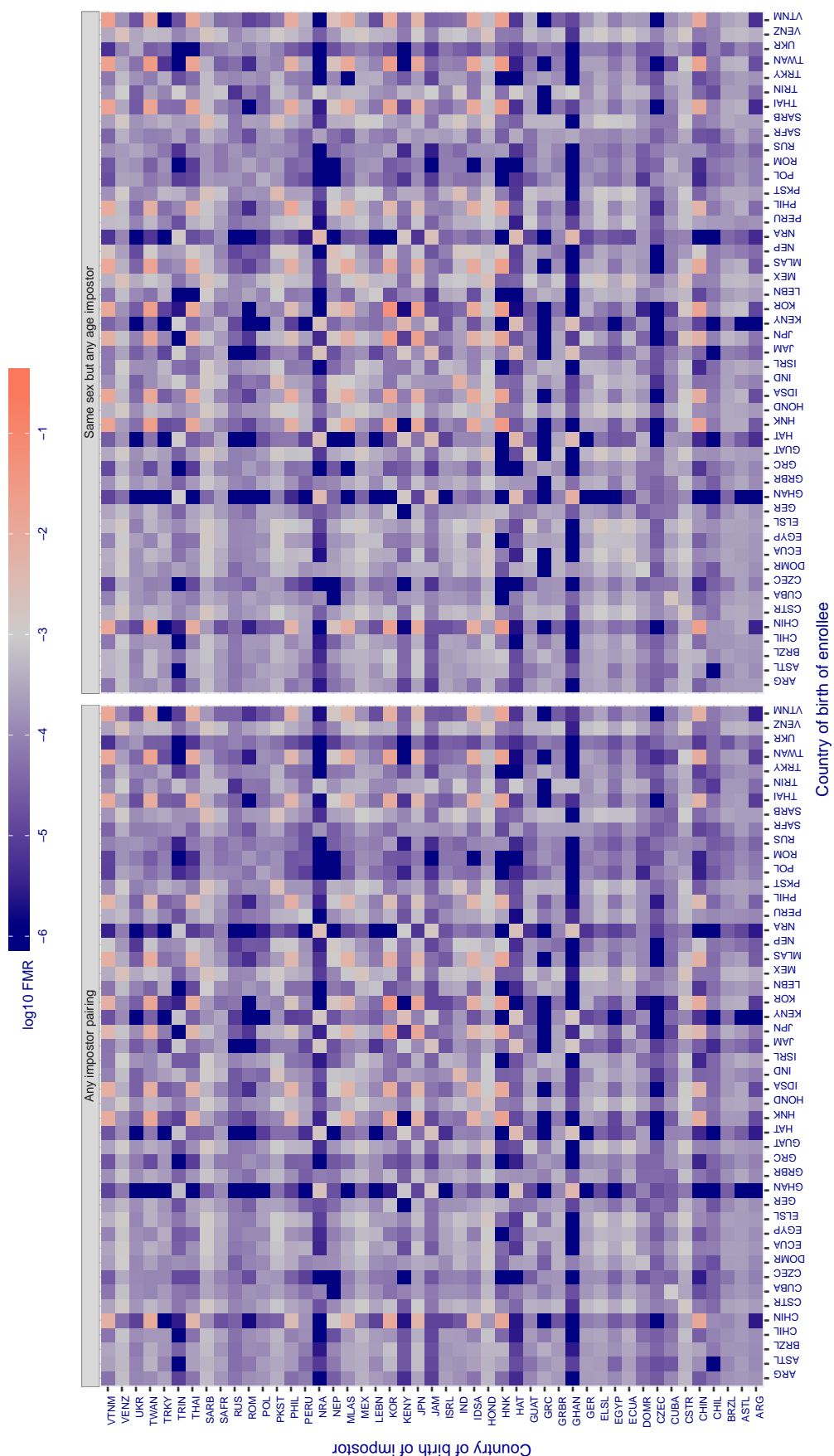


Figure 89: For algorithm id3-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 45.265$ for algorithm innovatrics_000, giving $FMR(T) = 0.001$ globally.

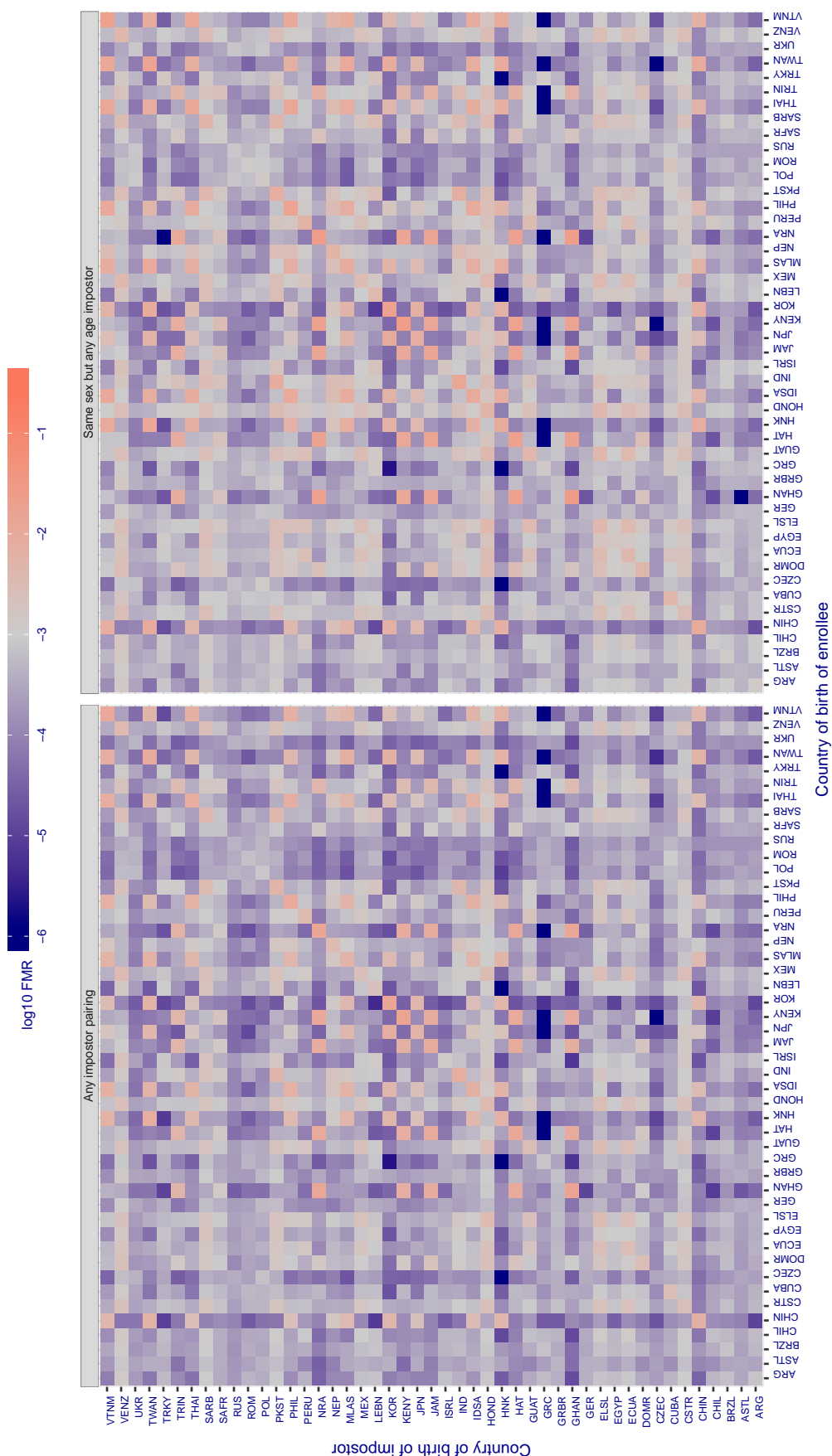


Figure 90: For algorithm innovatrics-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 41.476$ for algorithm innovatrics_001, giving $FMR(T) = 0.001$ globally.

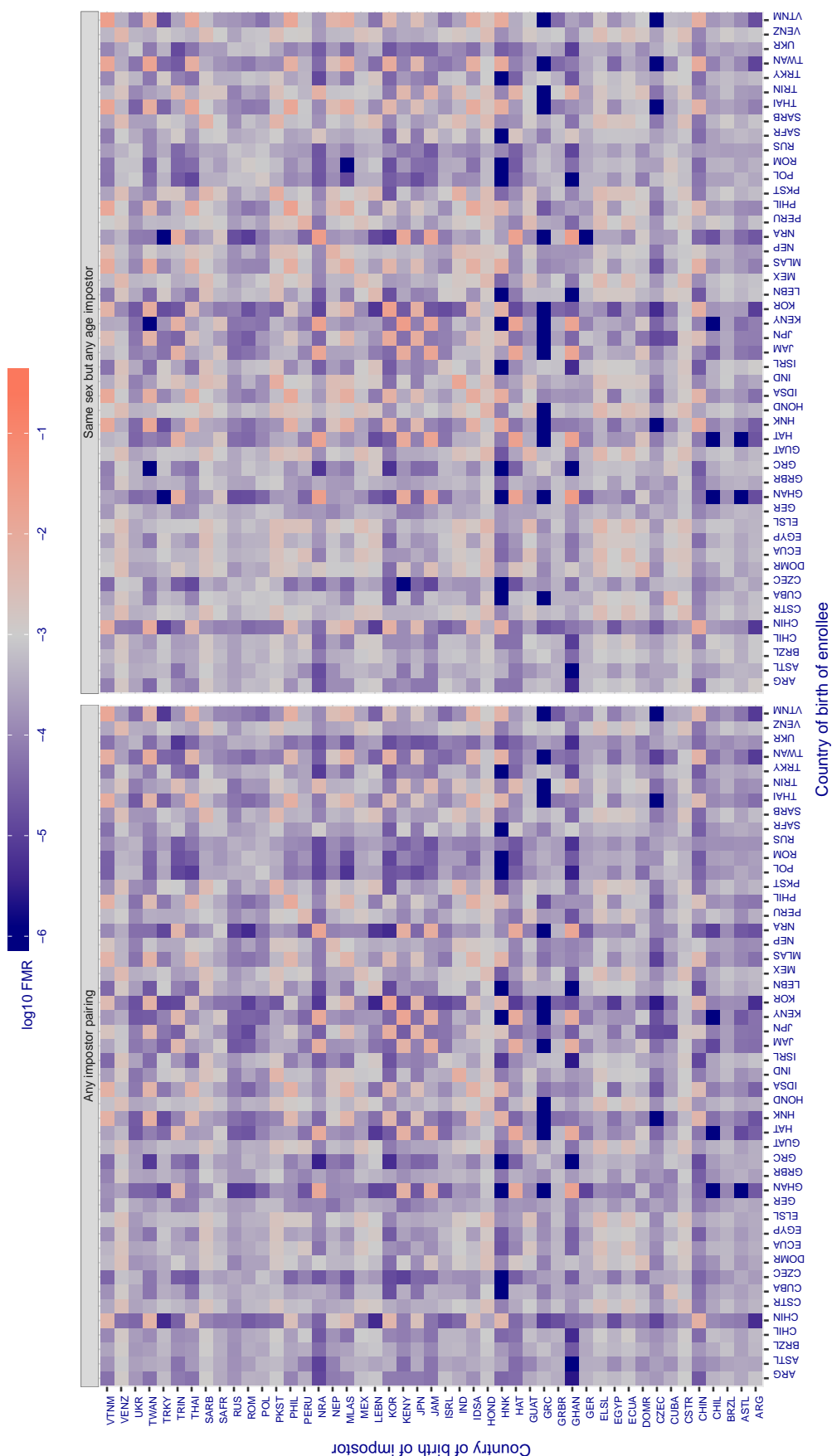


Figure 91: For algorithm innovatrics-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 37.554$ for algorithm intellivision_001, giving $FMR(T) = 0.001$ globally.

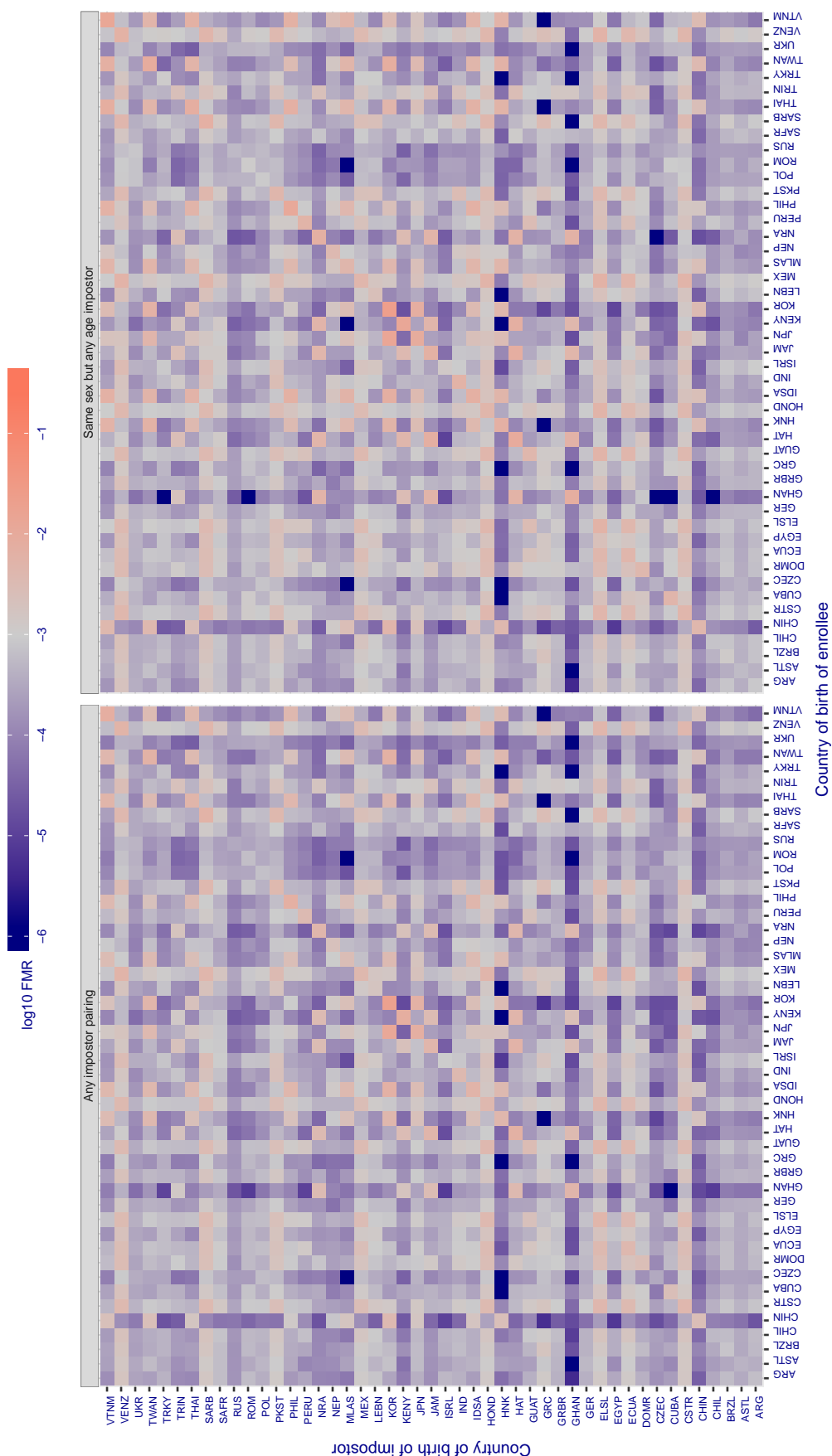


Figure 92: For algorithm intellivision-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

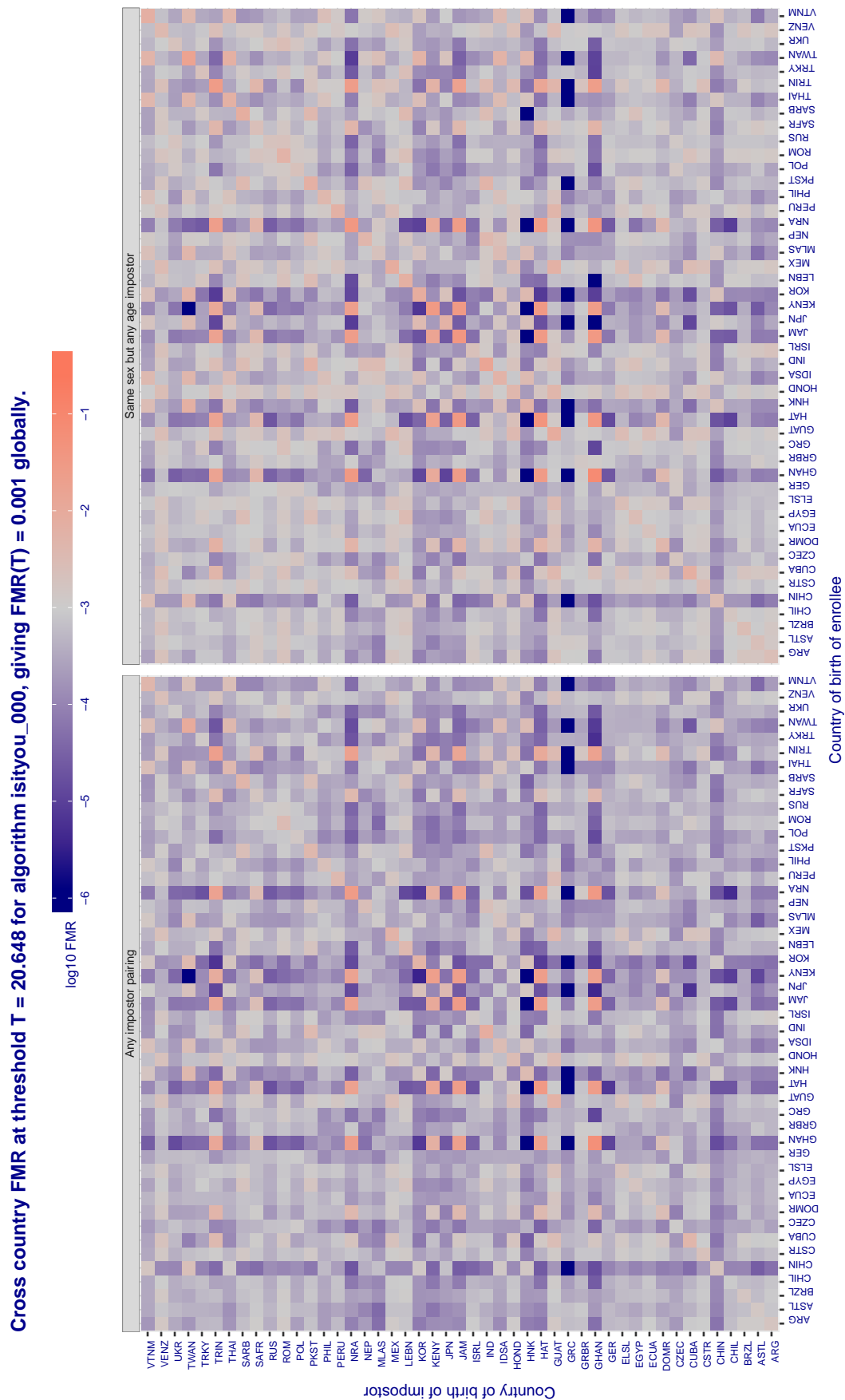
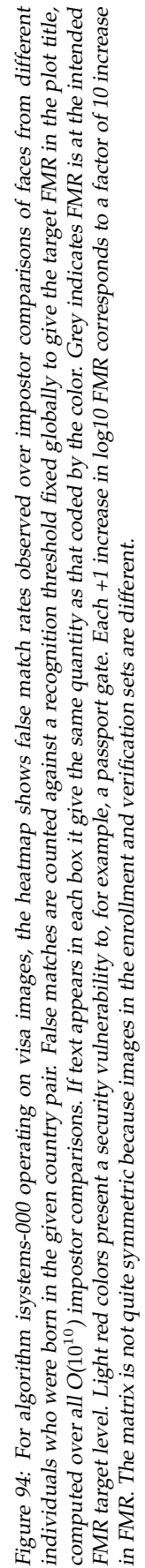


Figure 93: For algorithm isityou-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



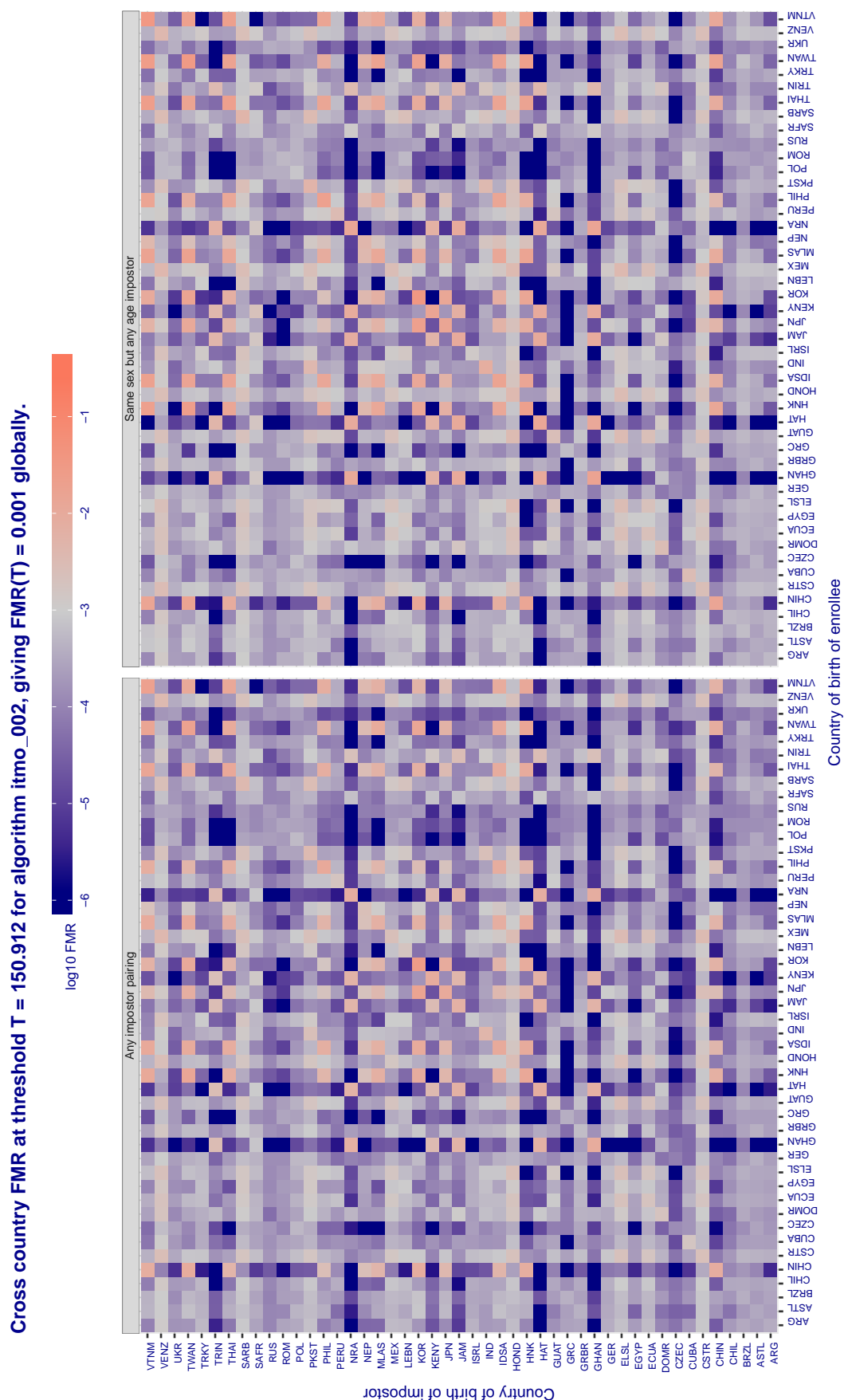


Figure 95: For algorithm itmo-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log₁₀ FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 3286.472$ for algorithm morpho_000, giving $FMR(T) = 0.001$ globally.

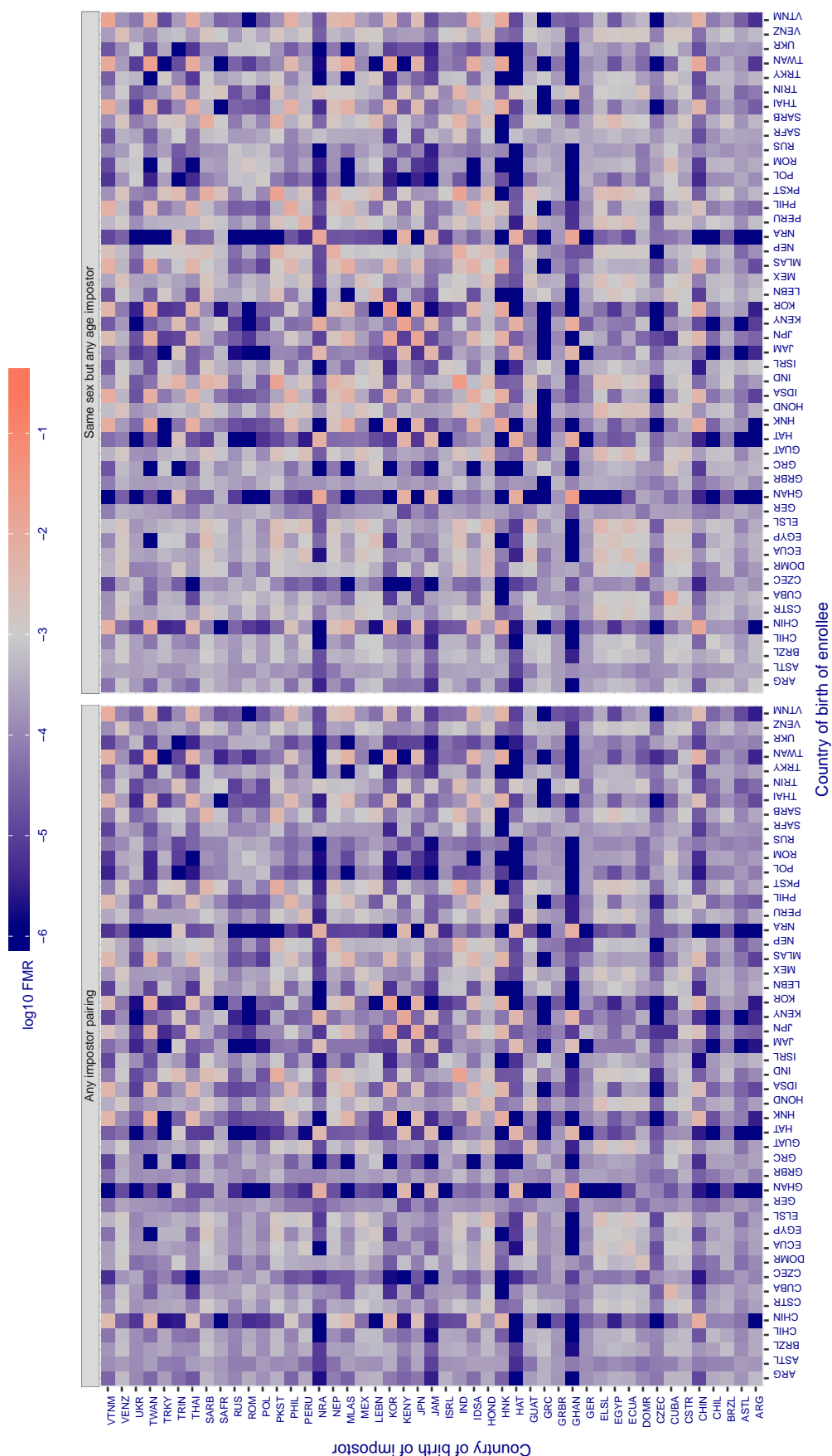
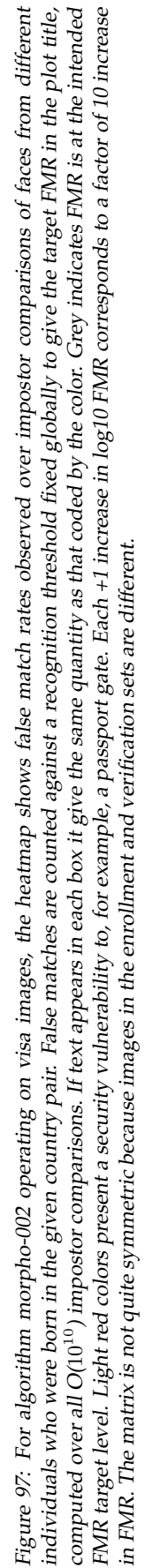


Figure 96: For algorithm morpho-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.



Cross country FMR at threshold $T = 32.150$ for algorithm neurotechnology_001, giving $FMR(T) = 0.001$ globally.

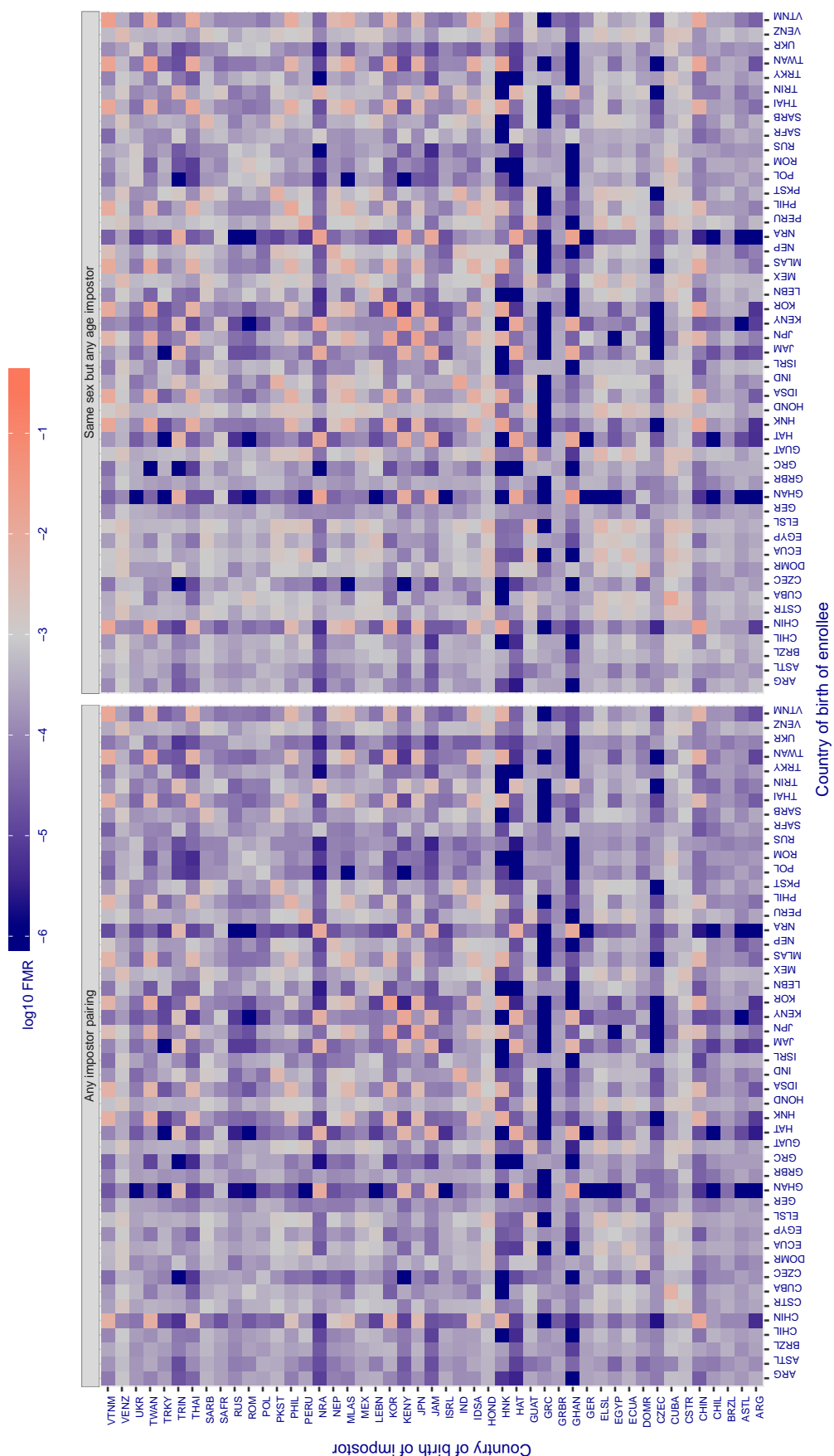


Figure 98: For algorithm neurotechnology-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each $+1$ increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 31.100$ for algorithm neurotechnology_002, giving $FMR(T) = 0.001$ globally.

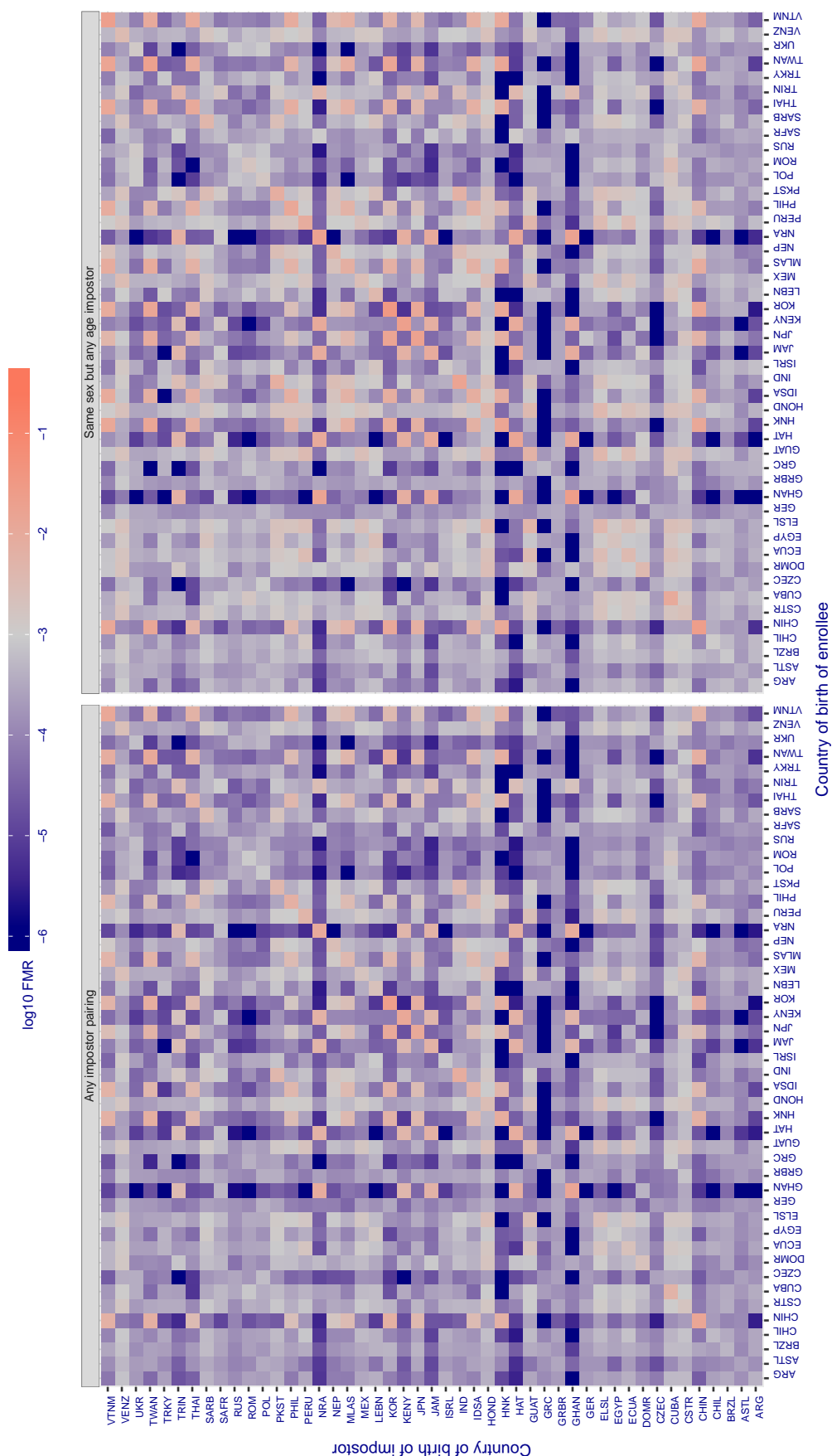


Figure 99: For algorithm neurotechnology-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log₁₀ FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

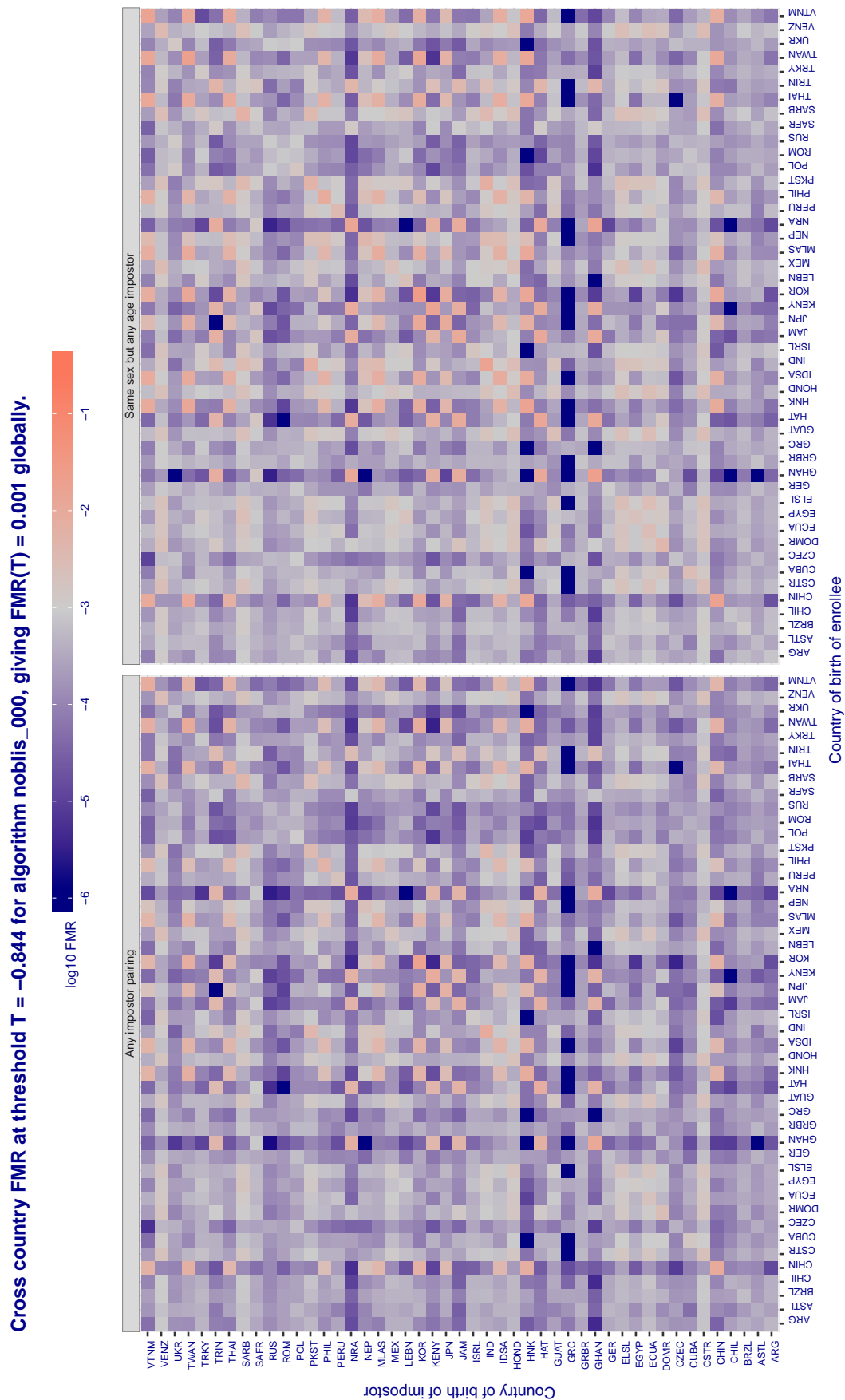


Figure 100: For algorithm nobilis-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log₁₀ FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

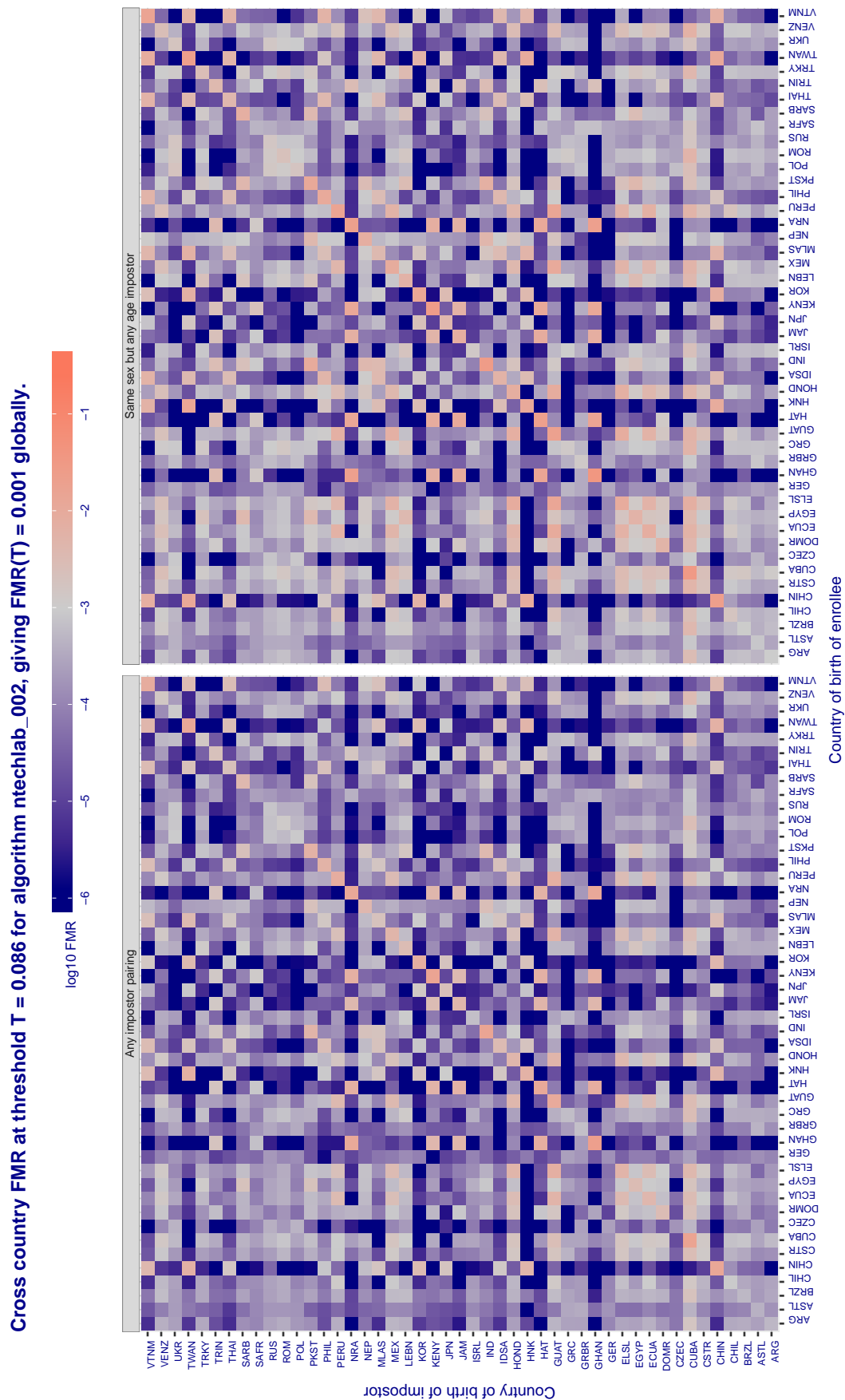


Figure 101: For algorithm ntechlab-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log₁₀ FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 2.947$ for algorithm ntechlab_003, giving $FMR(T) = 0.001$ globally.

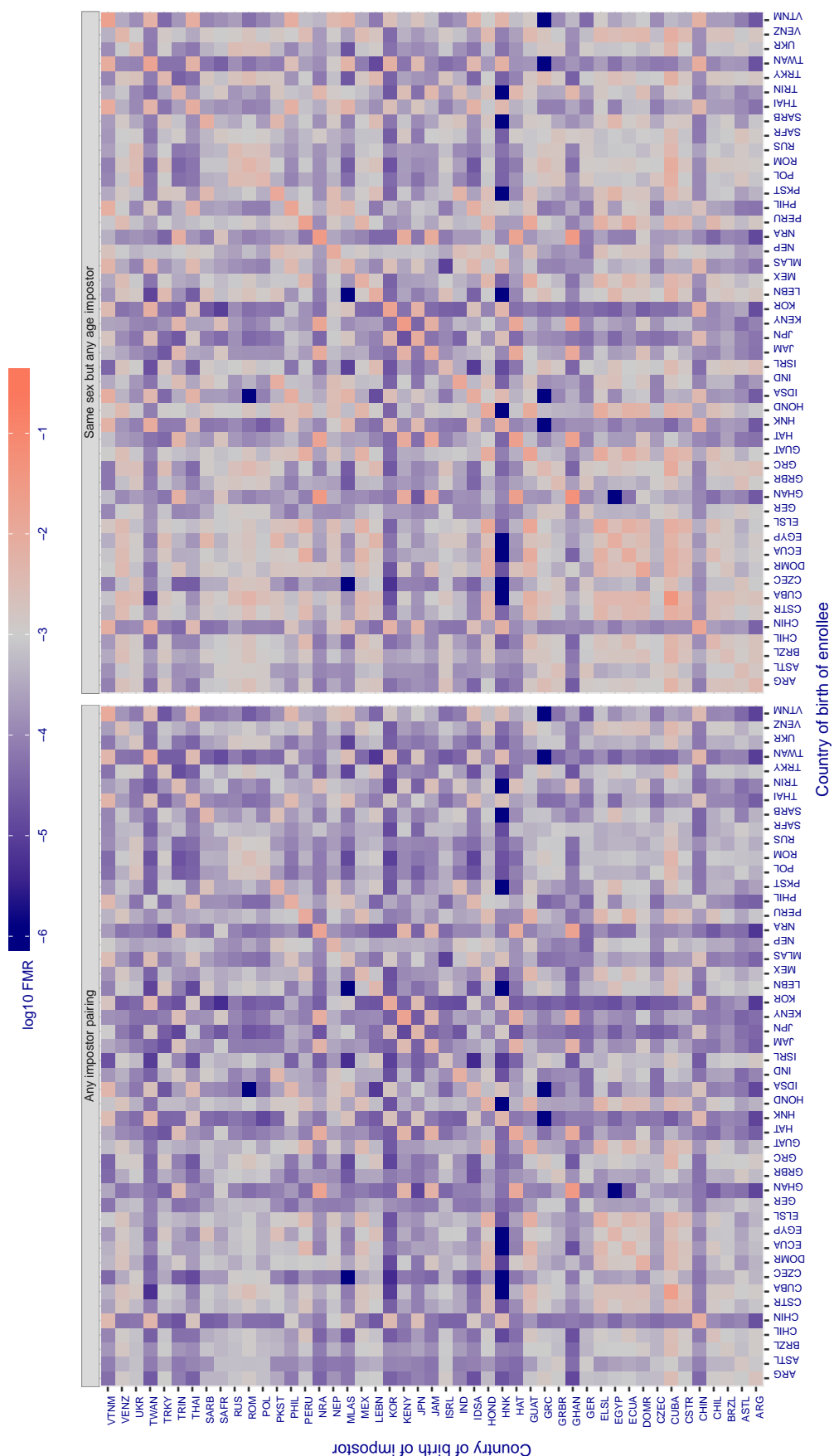


Figure 102: For algorithm ntechlab-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each $+1$ increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 0.795$ for algorithm pa_002, giving $FMR(T) = 0.001$ globally.

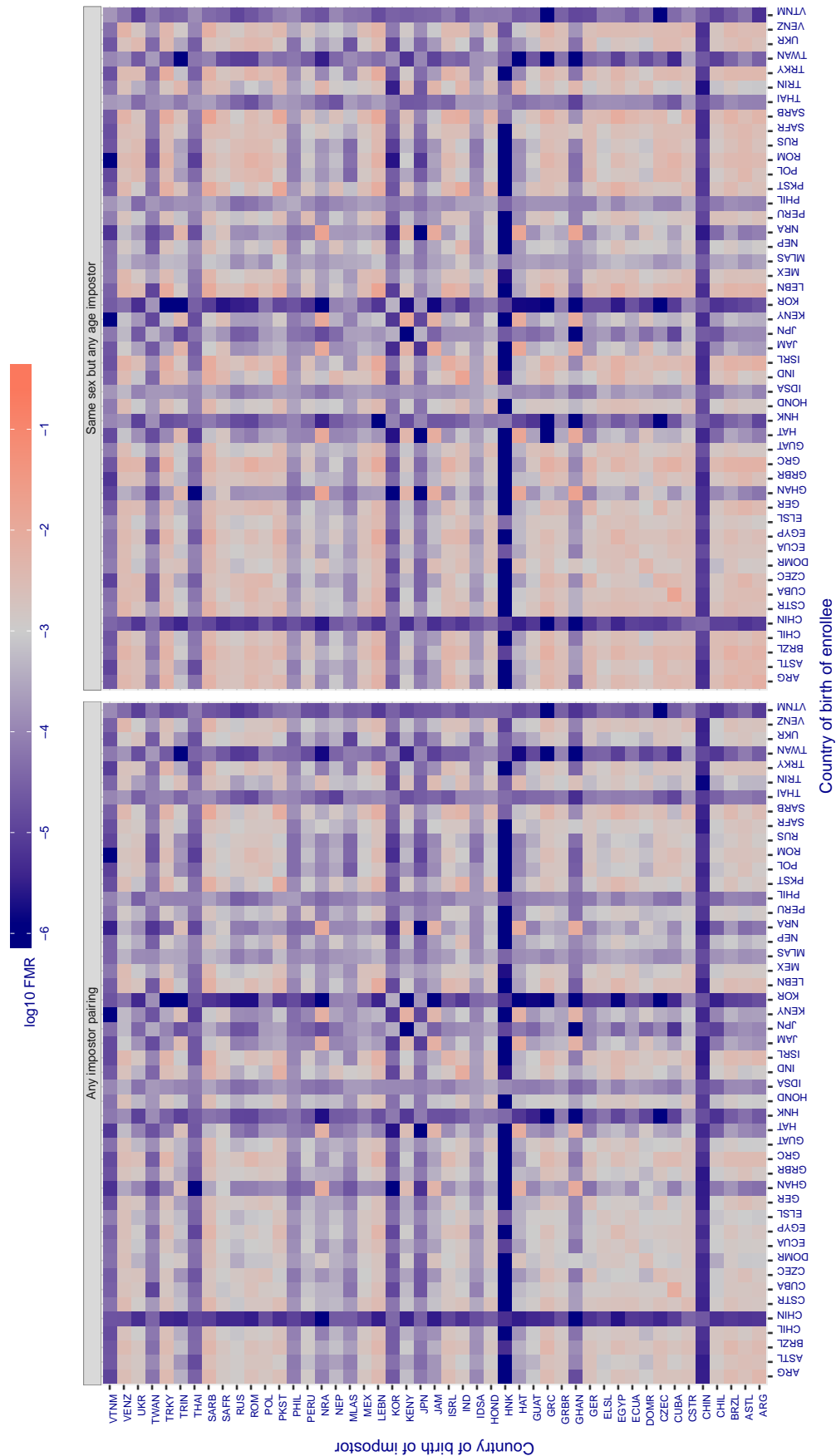


Figure 103: For algorithm pa-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

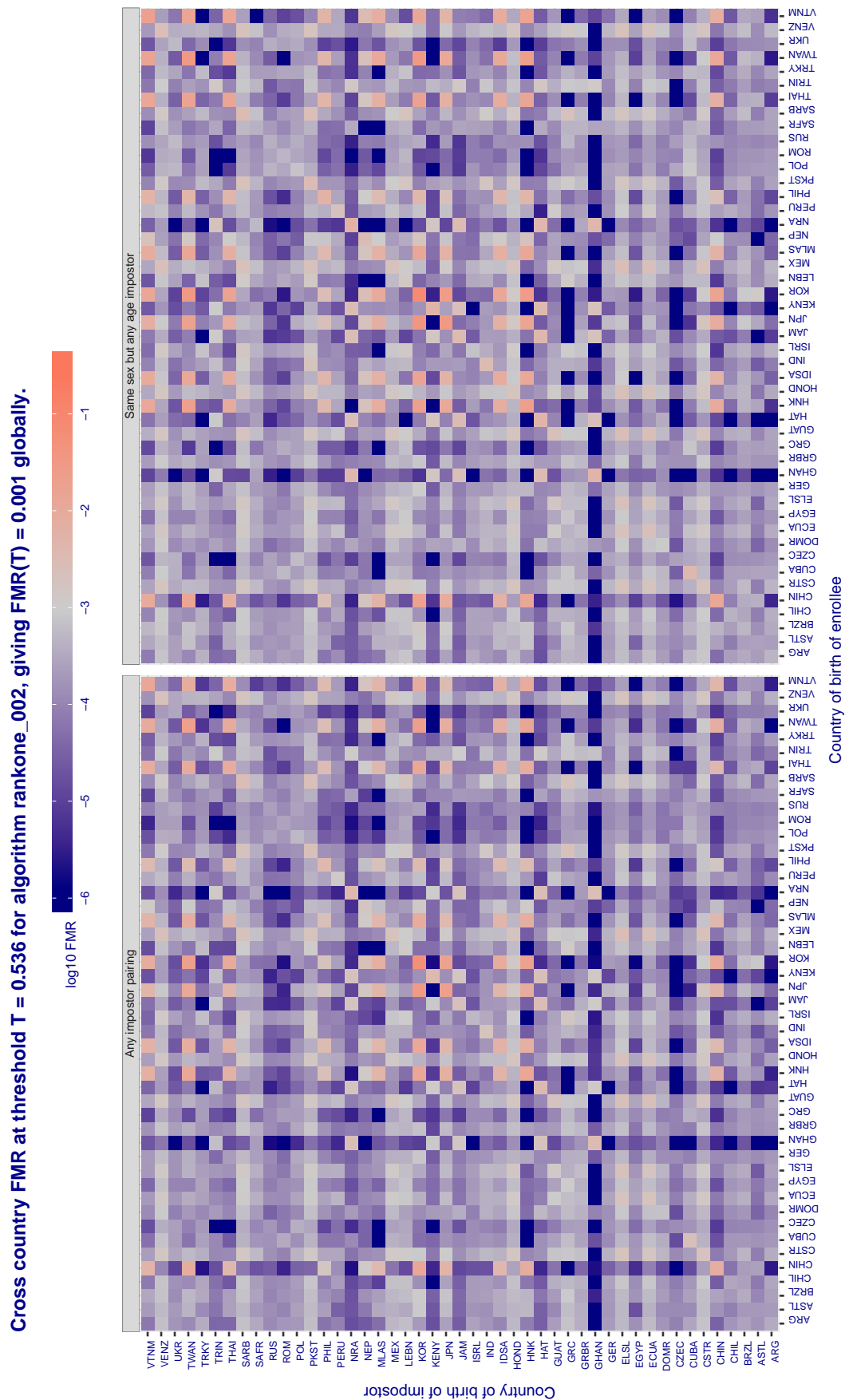


Figure 104: For algorithm rankone-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 0.585$ for algorithm rankone_003, giving $FMR(T) = 0.001$ globally.

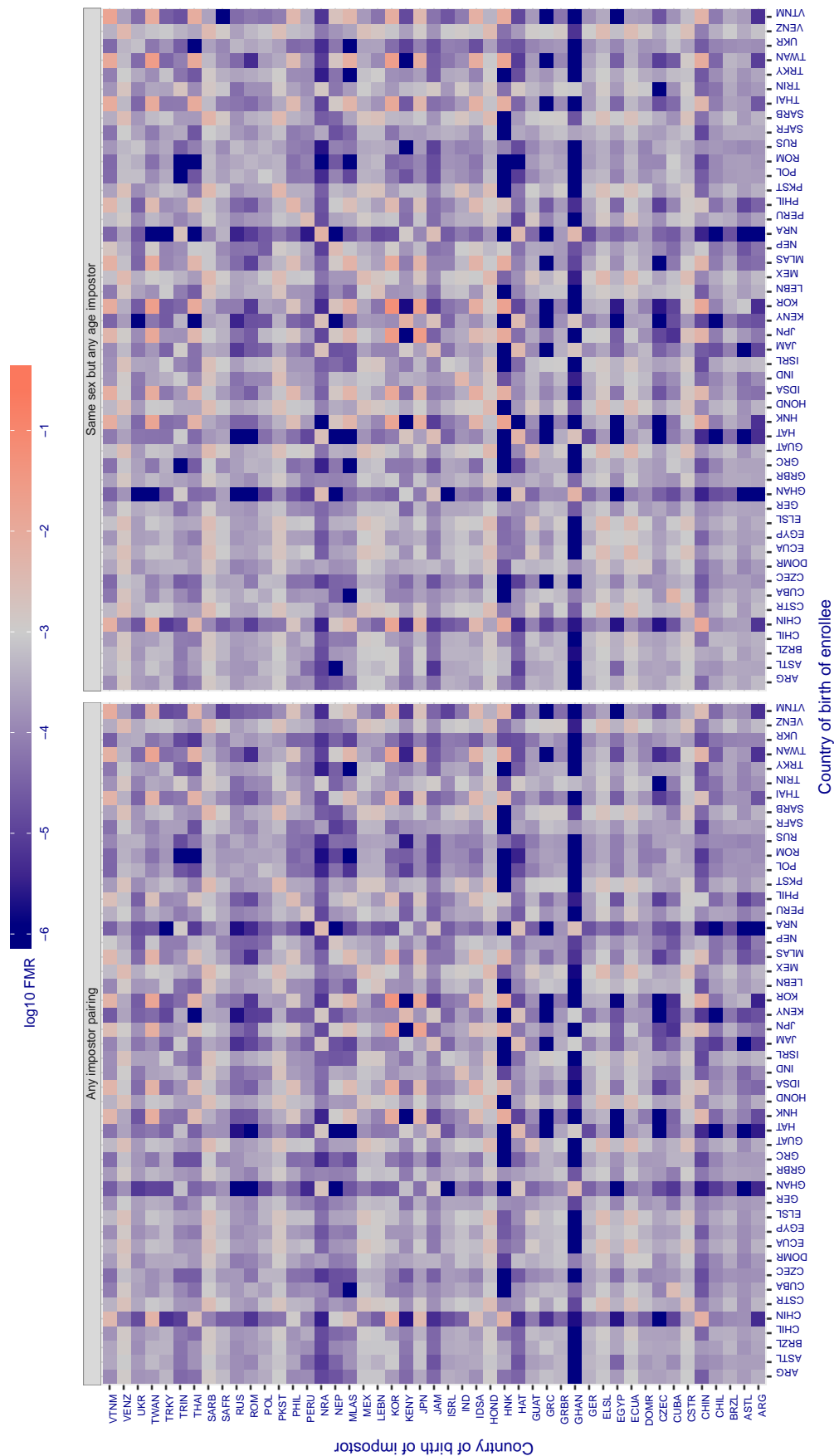


Figure 105: For algorithm rankone-003 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

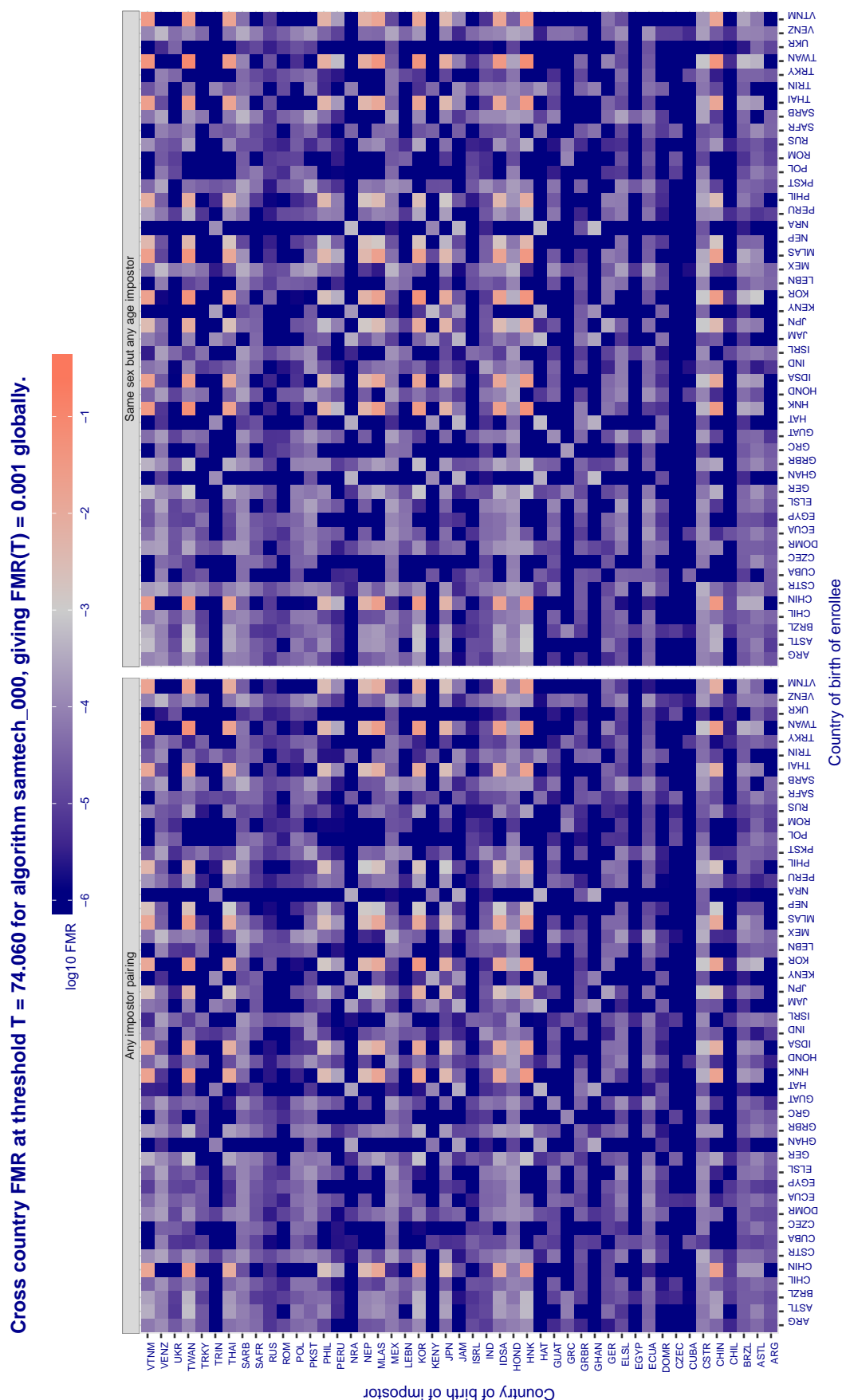


Figure 106: For algorithm samtech-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log₁₀ FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 0.939$ for algorithm shaman_000, giving $FMR(T) = 0.001$ globally.

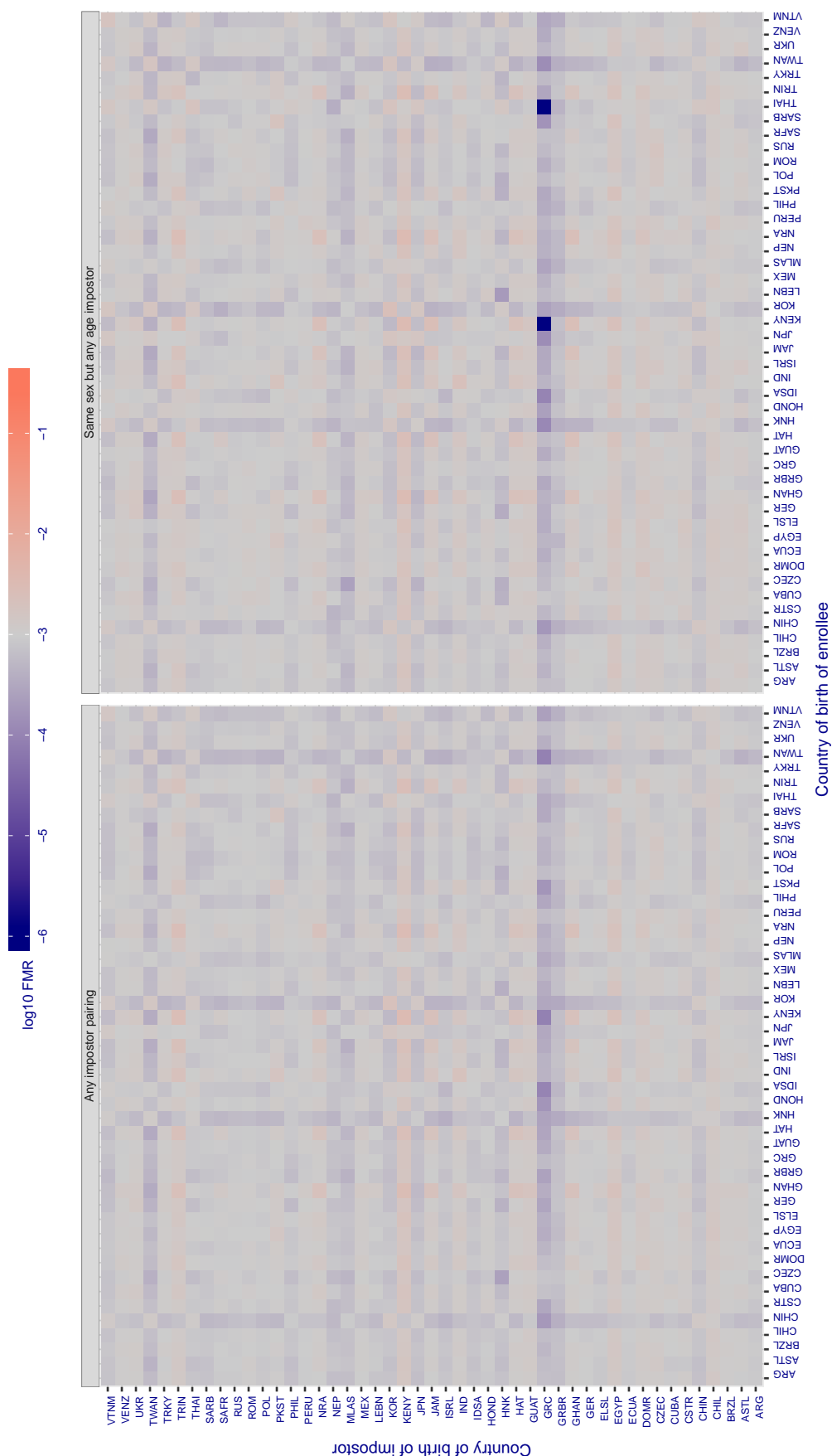


Figure 107: For algorithm shaman-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

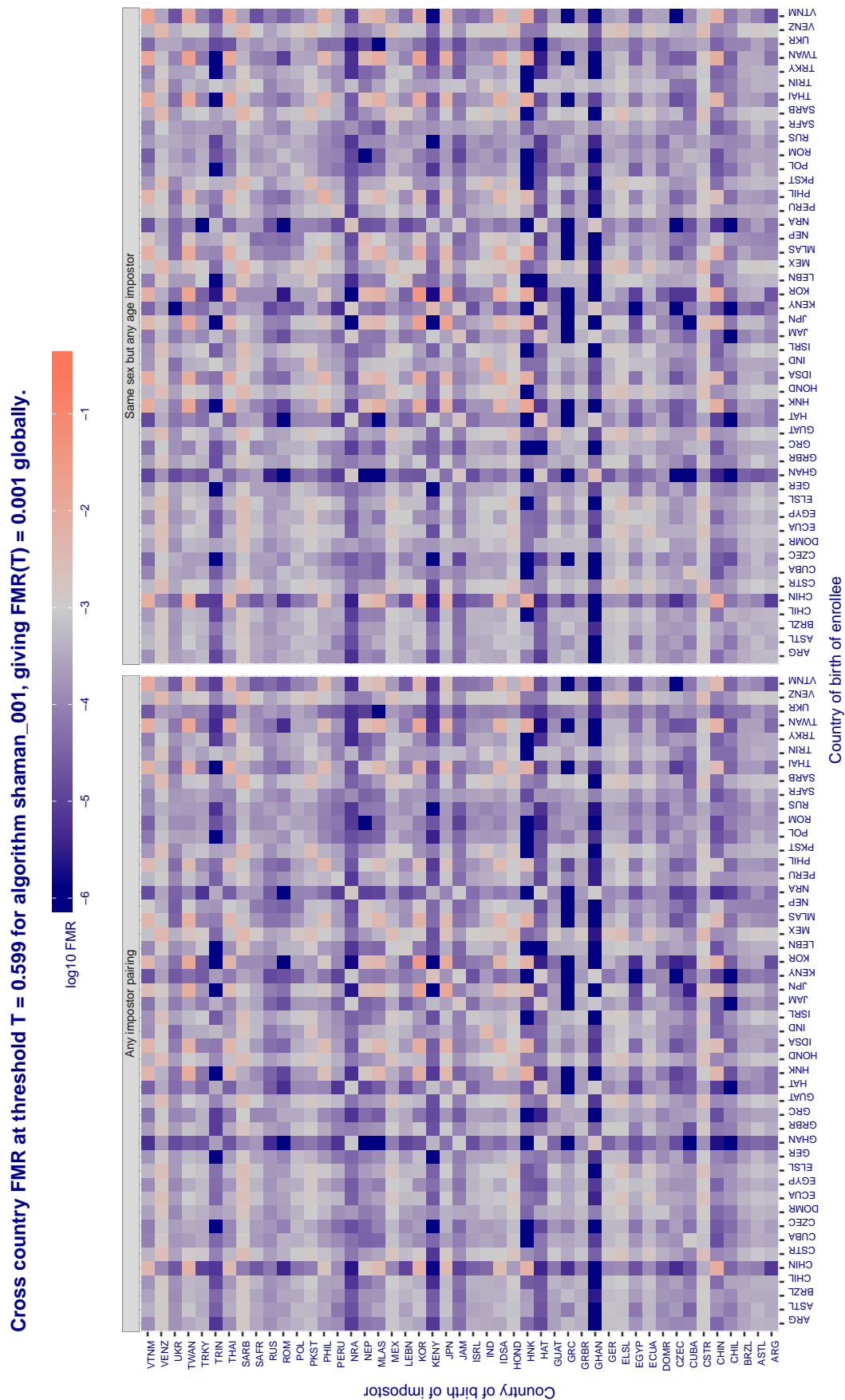


Figure 108: For algorithm shaman-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log10 FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

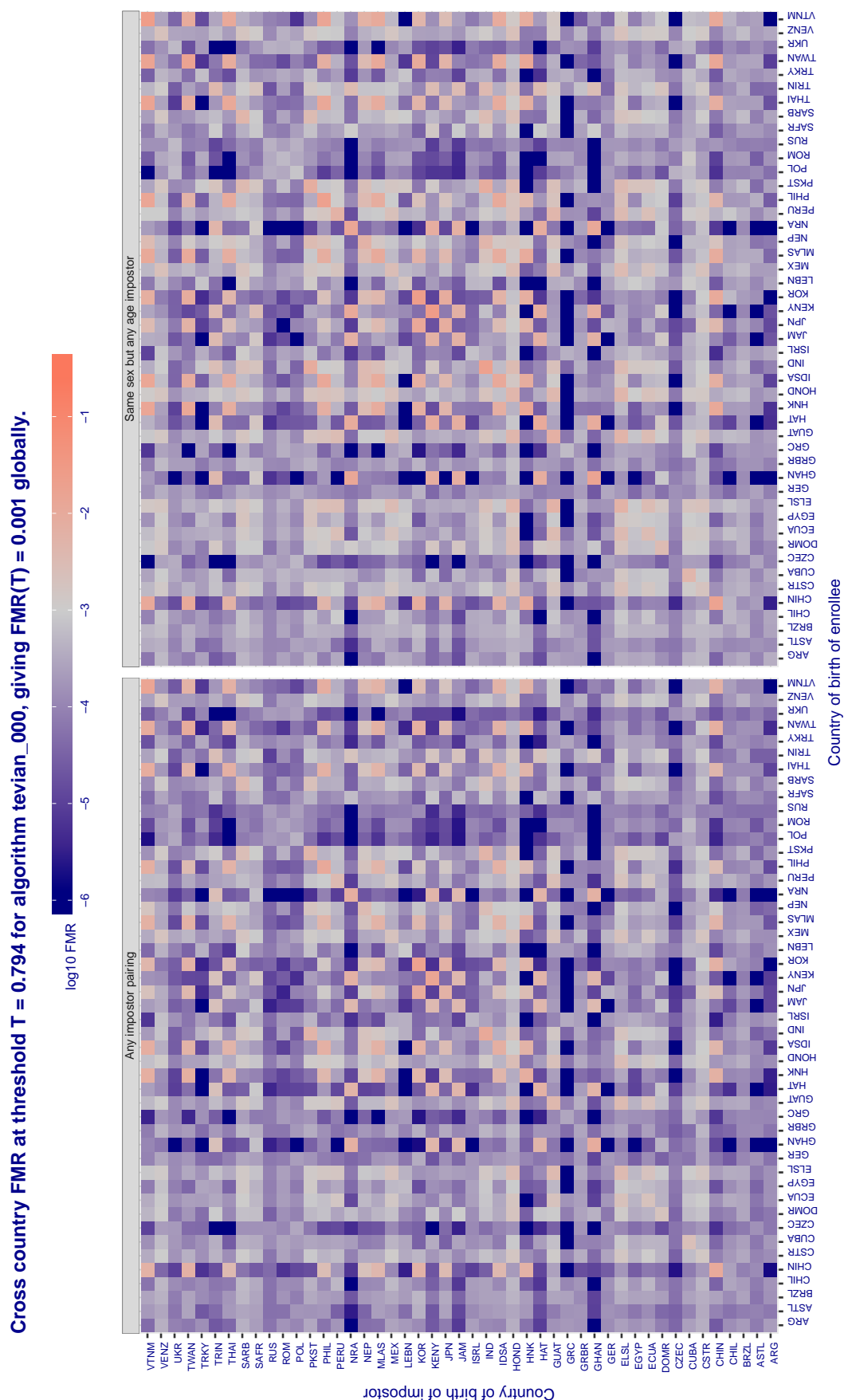


Figure 109: For algorithm `tevian-000` operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each $+1$ increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 9.972$ for algorithm tongyitrans_001, giving $FMR(T) = 0.001$ globally.

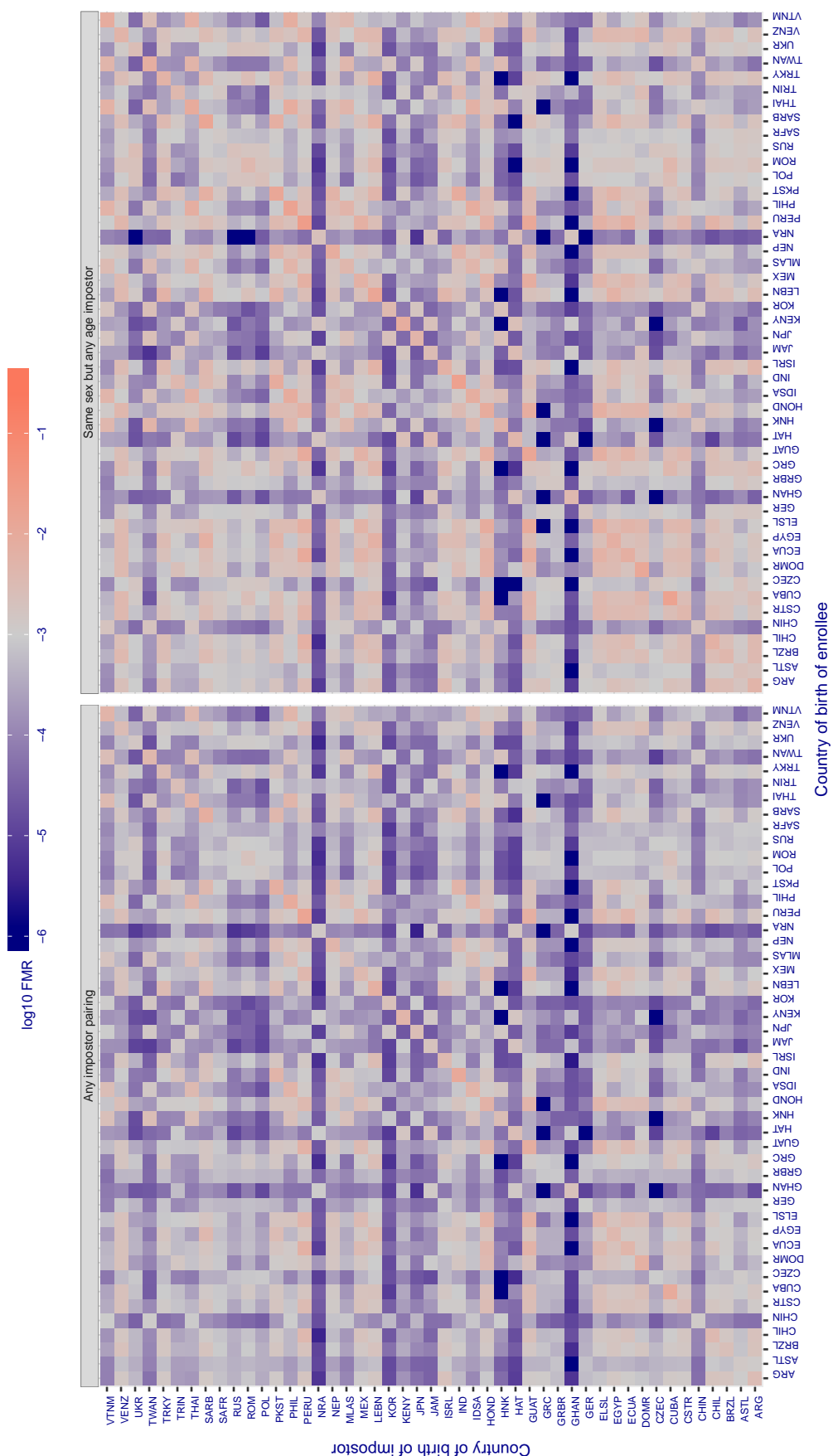


Figure 110: For algorithm tongyitrans-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 3.810$ for algorithm tongyitrans_002, giving $FMR(T) = 0.001$ globally.

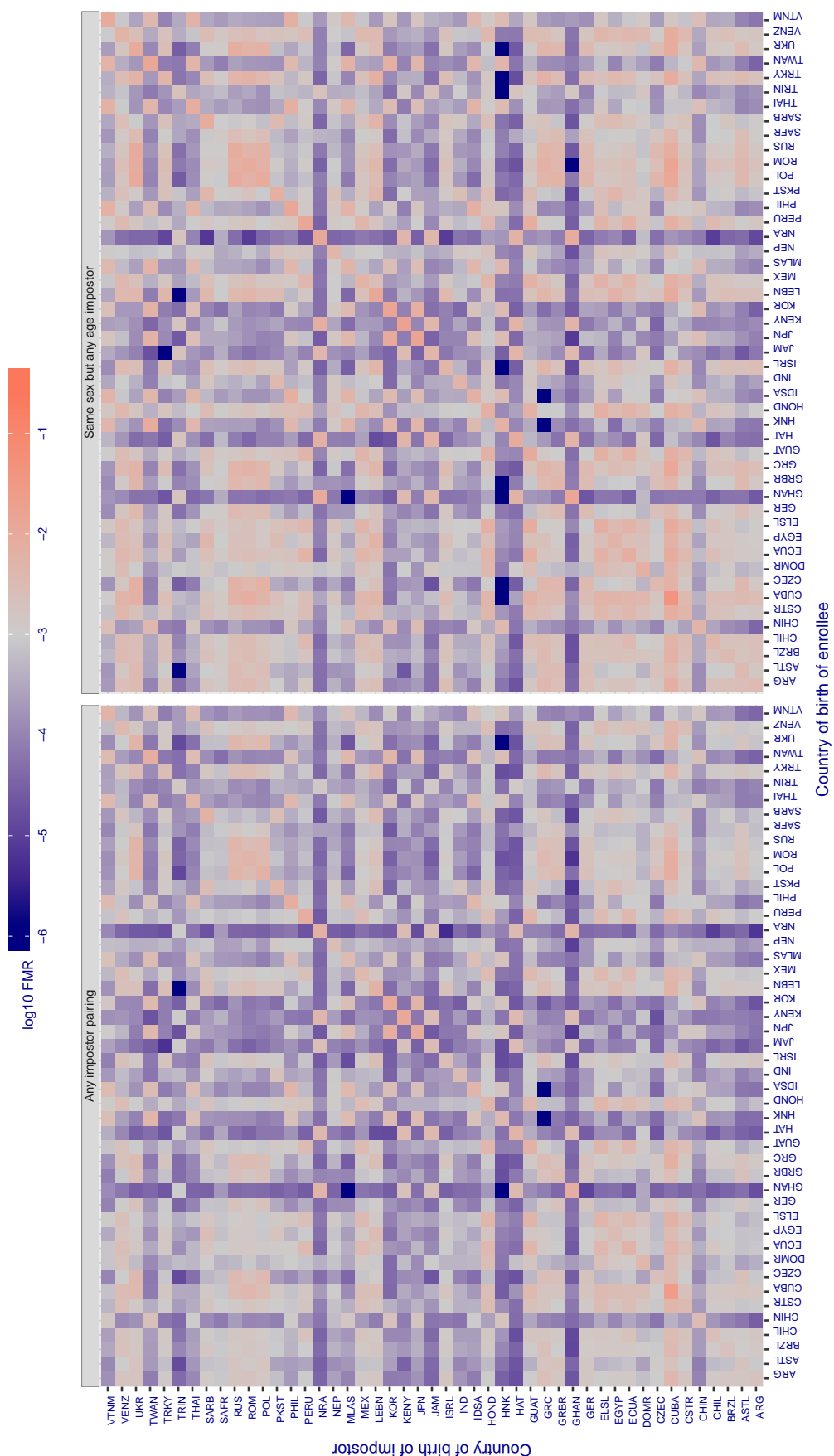


Figure 111: For algorithm tongyitrans-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

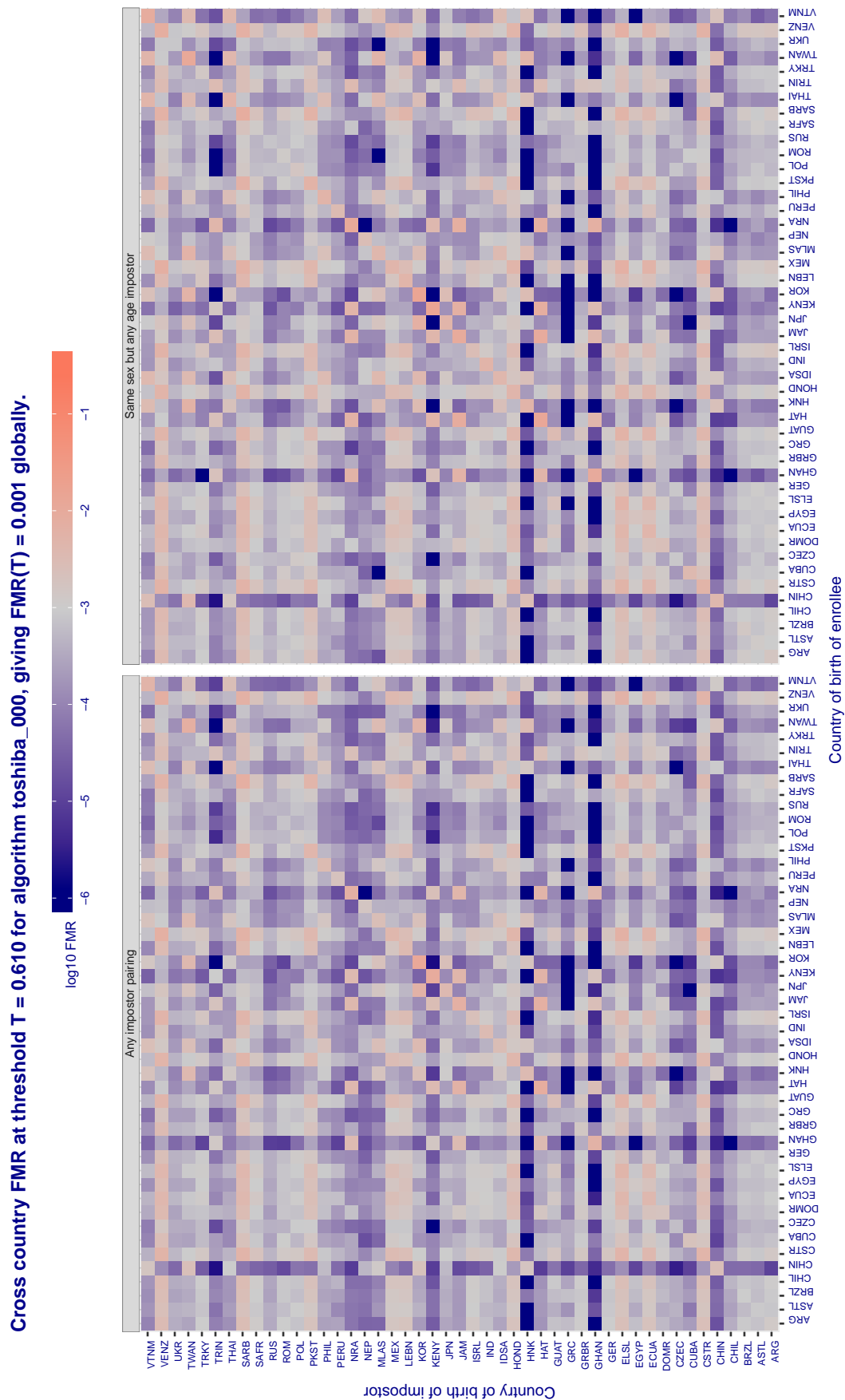


Figure 112: For algorithm toshiba-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log₁₀ FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 0.579$ for algorithm toshiba_001, giving $FMR(T) = 0.001$ globally.

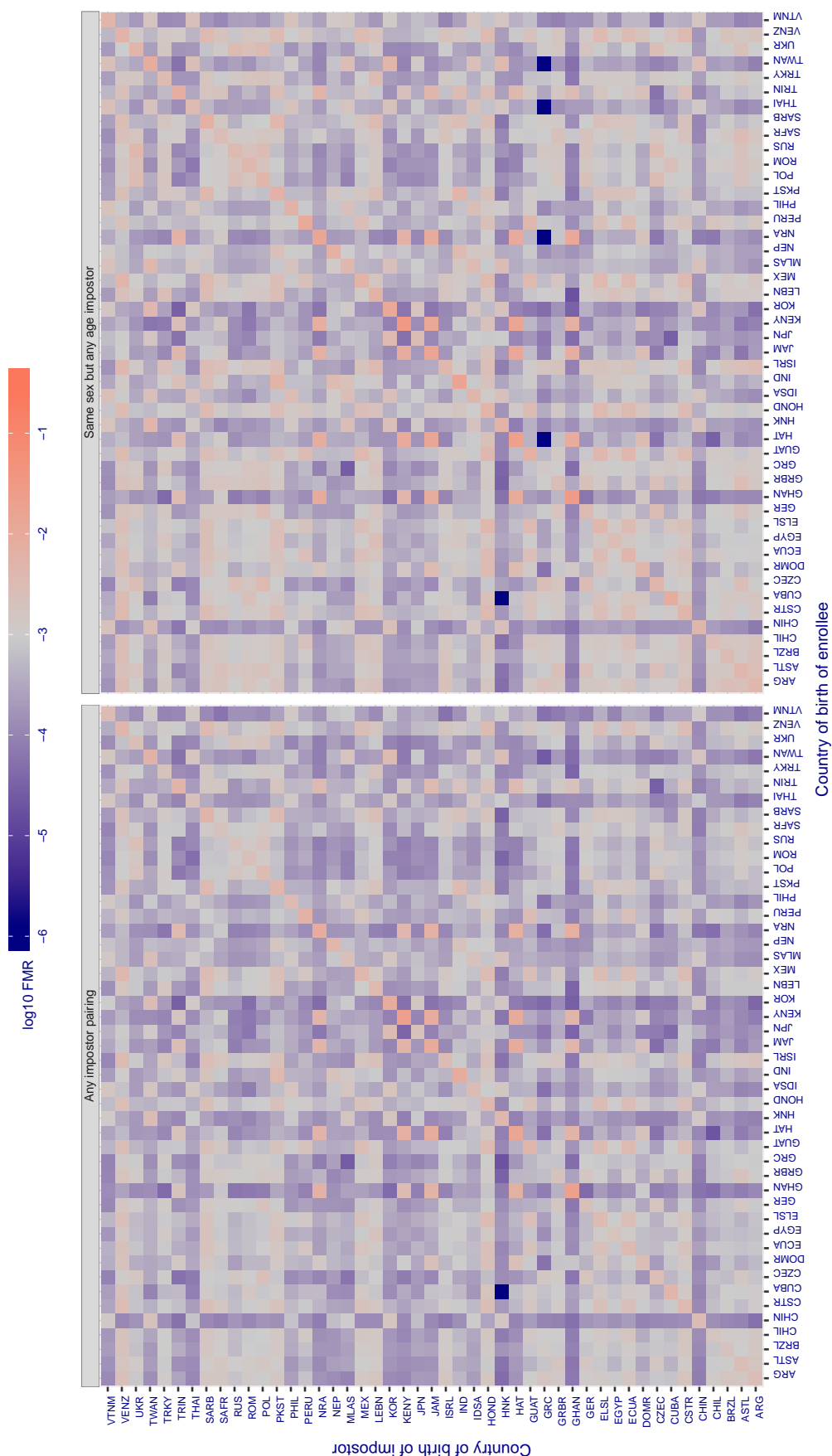
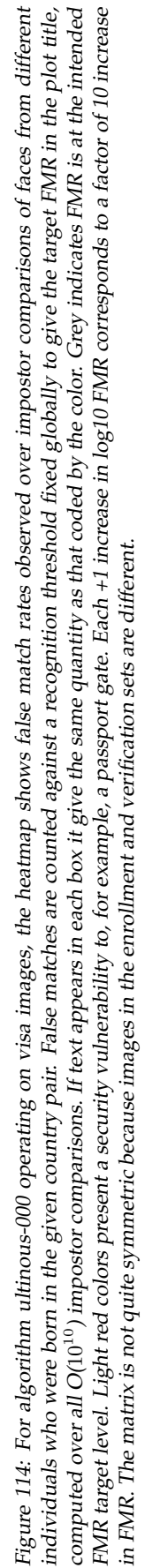
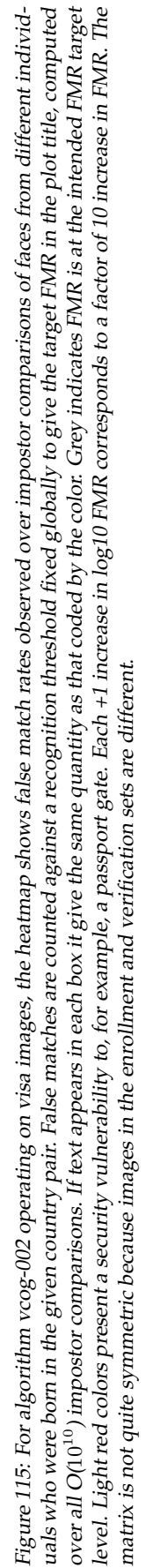


Figure 113: For algorithm toshiba-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.





Cross country FMR at threshold $T = 4.153$ for algorithm vigilantsolutions_002, giving $FMR(T) = 0.001$ globally.

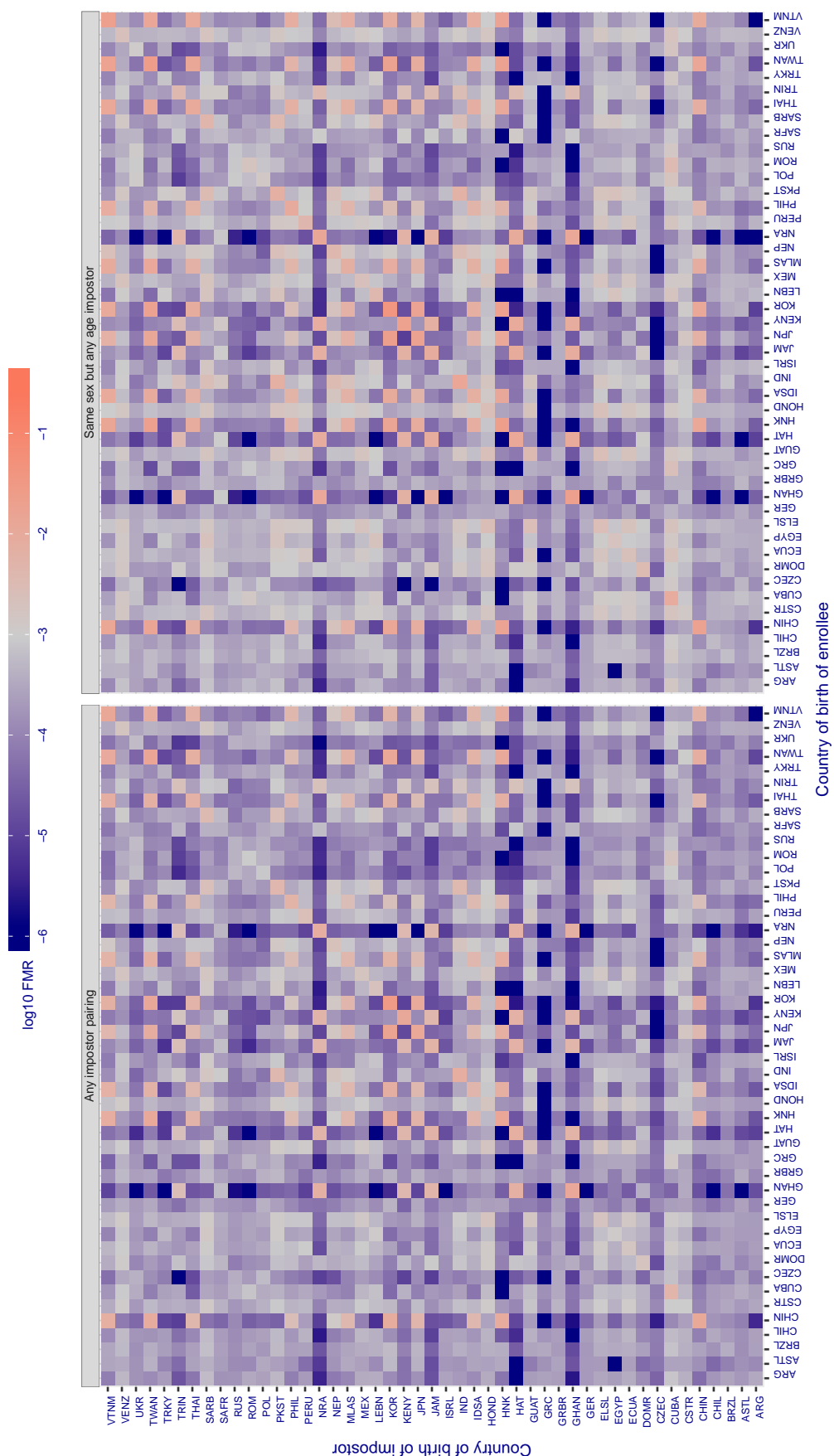


Figure 116: For algorithm vigilantsolutions-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 0.009$ for algorithm visionlabs_001, giving $FMR(T) = 0.001$ globally.

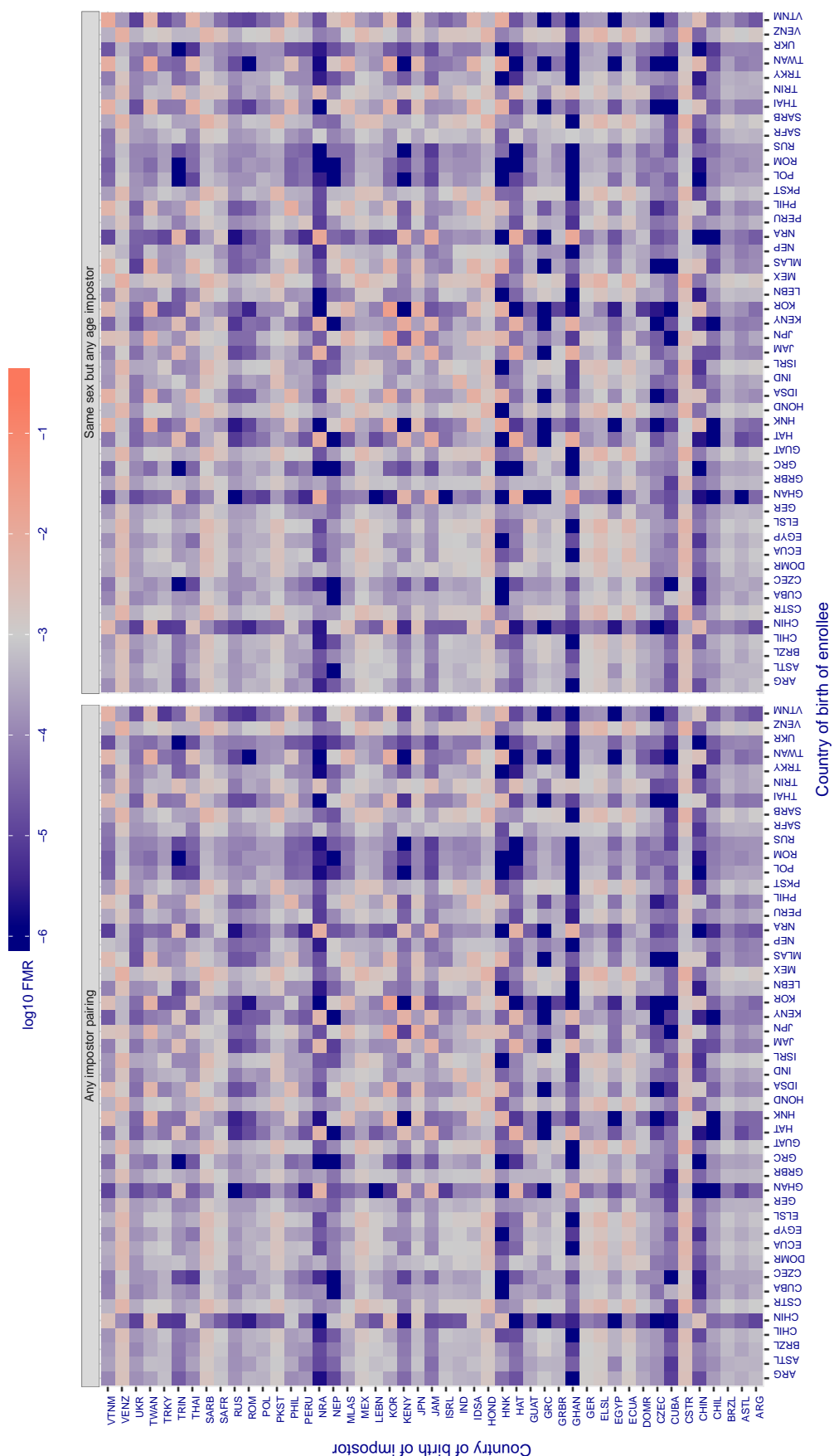


Figure 117: For algorithm visionlabs-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in \log_{10} FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 0.573$ for algorithm visionlabs_002, giving $FMR(T) = 0.001$ globally.

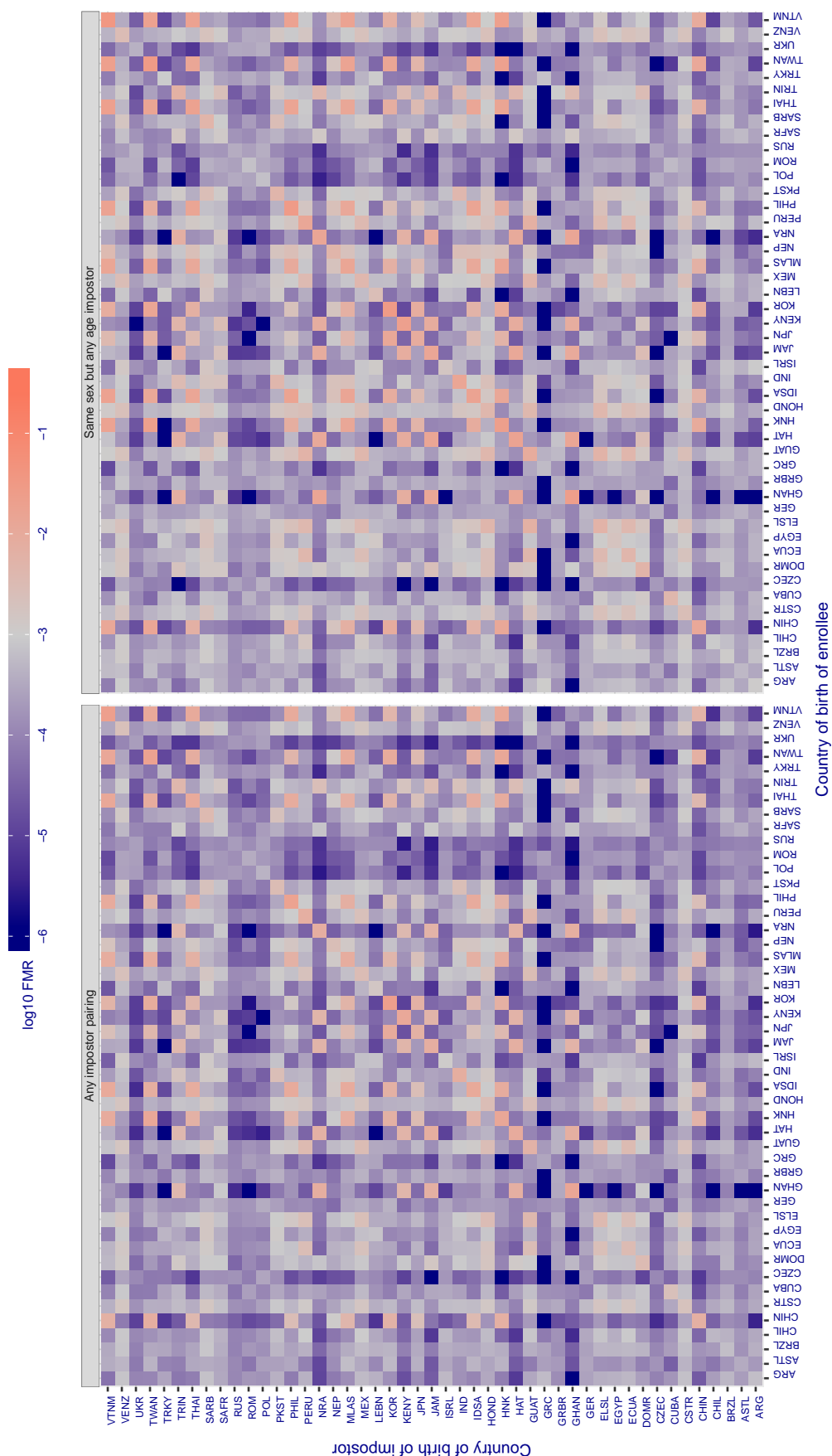


Figure 118: For algorithm visionlabs-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

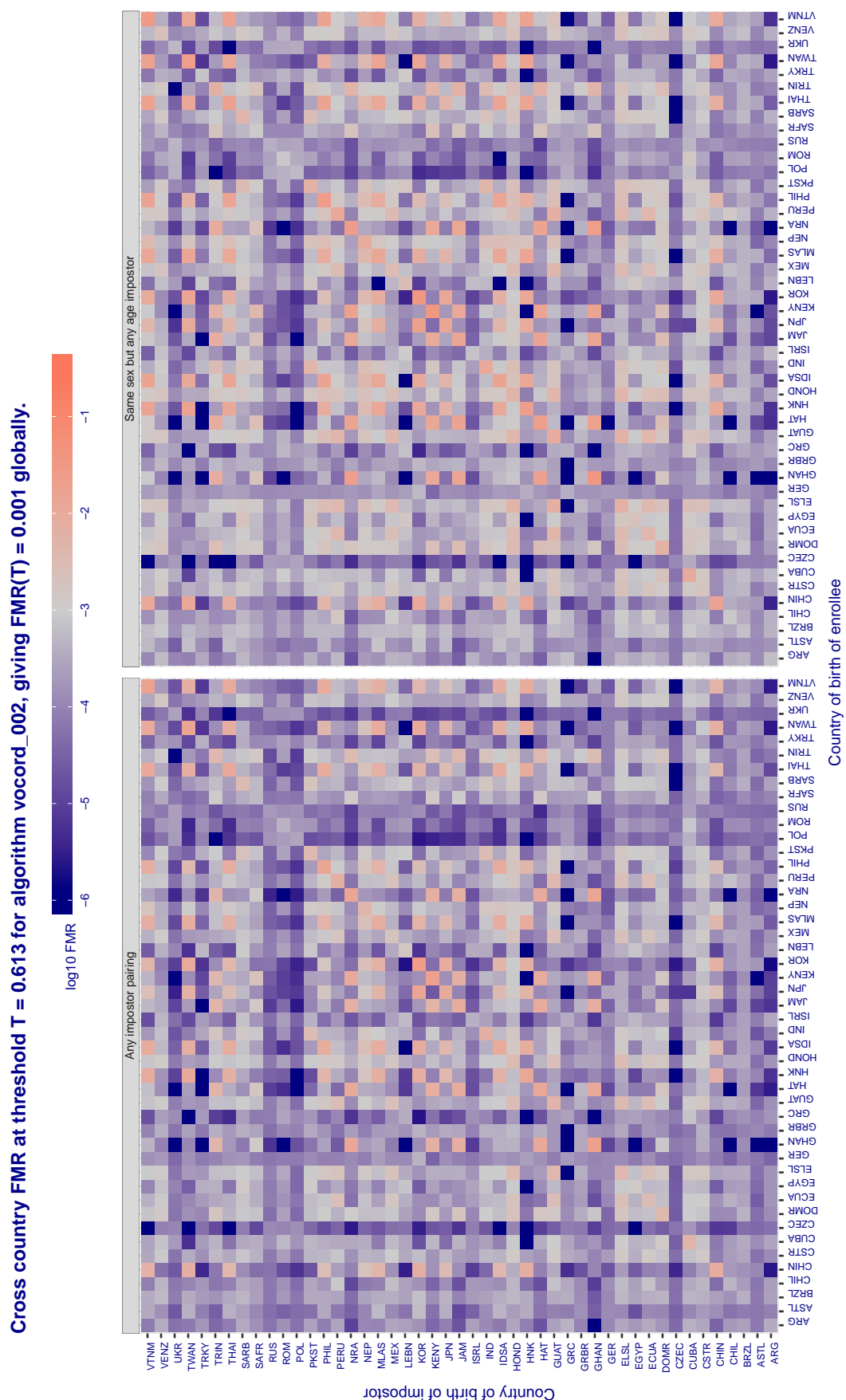


Figure 119: For algorithm vocord-002 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log₁₀ FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

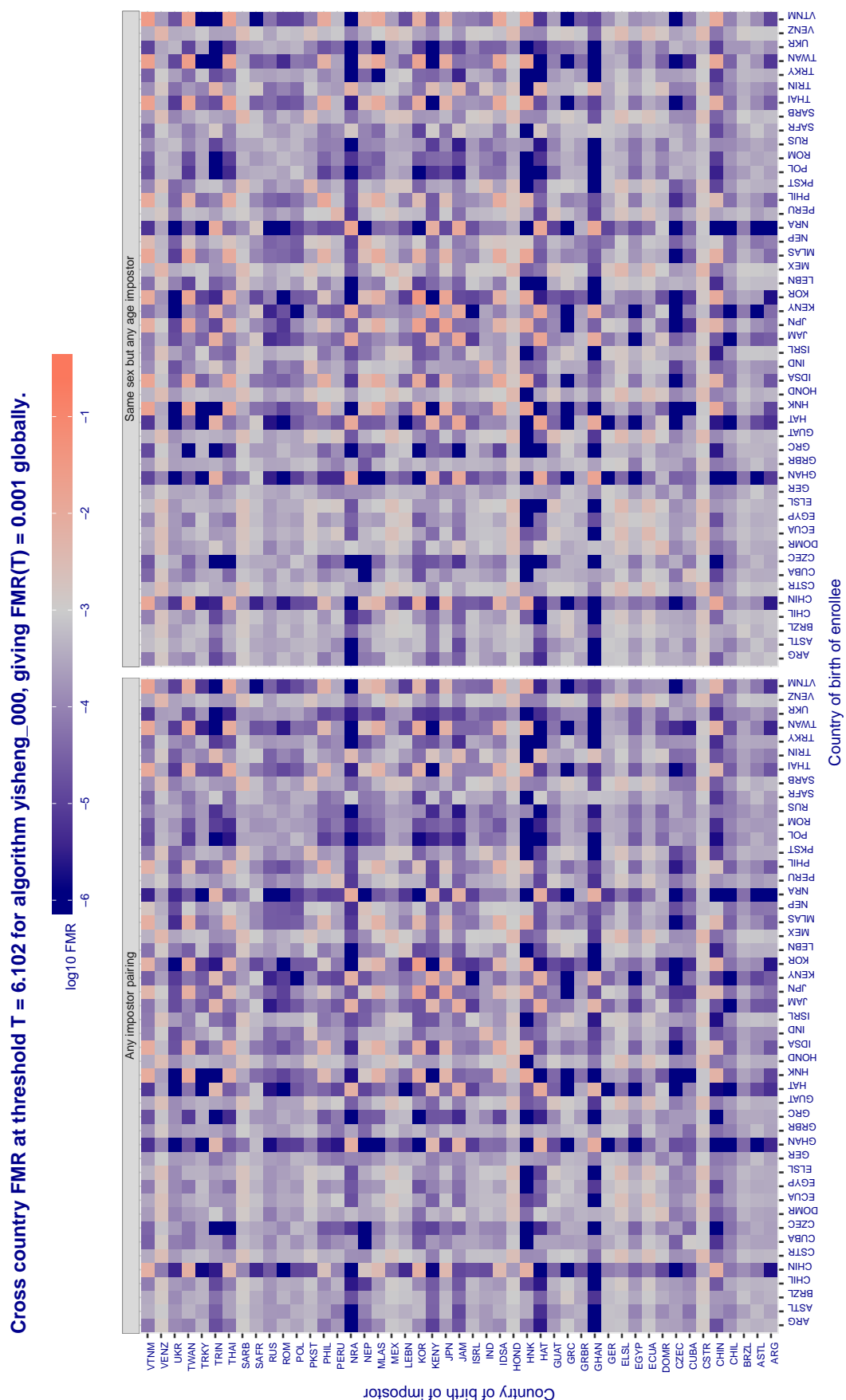


Figure 120: For algorithm yisheng-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log₁₀ FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

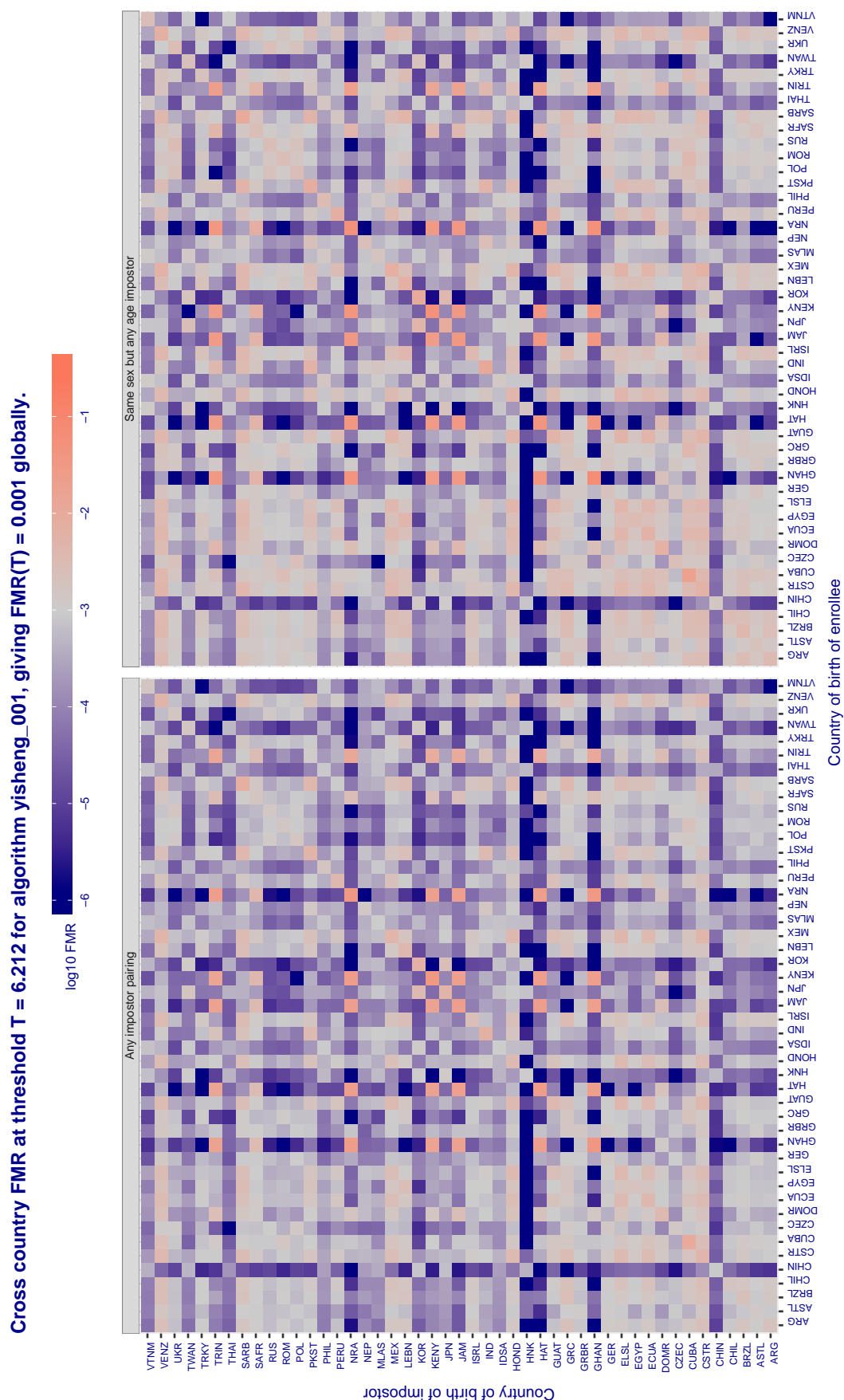


Figure 121: For algorithm yisheng-001 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in log₁₀ FMR corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

Cross country FMR at threshold $T = 9.942$ for algorithm yitu_000, giving $FMR(T) = 0.001$ globally.

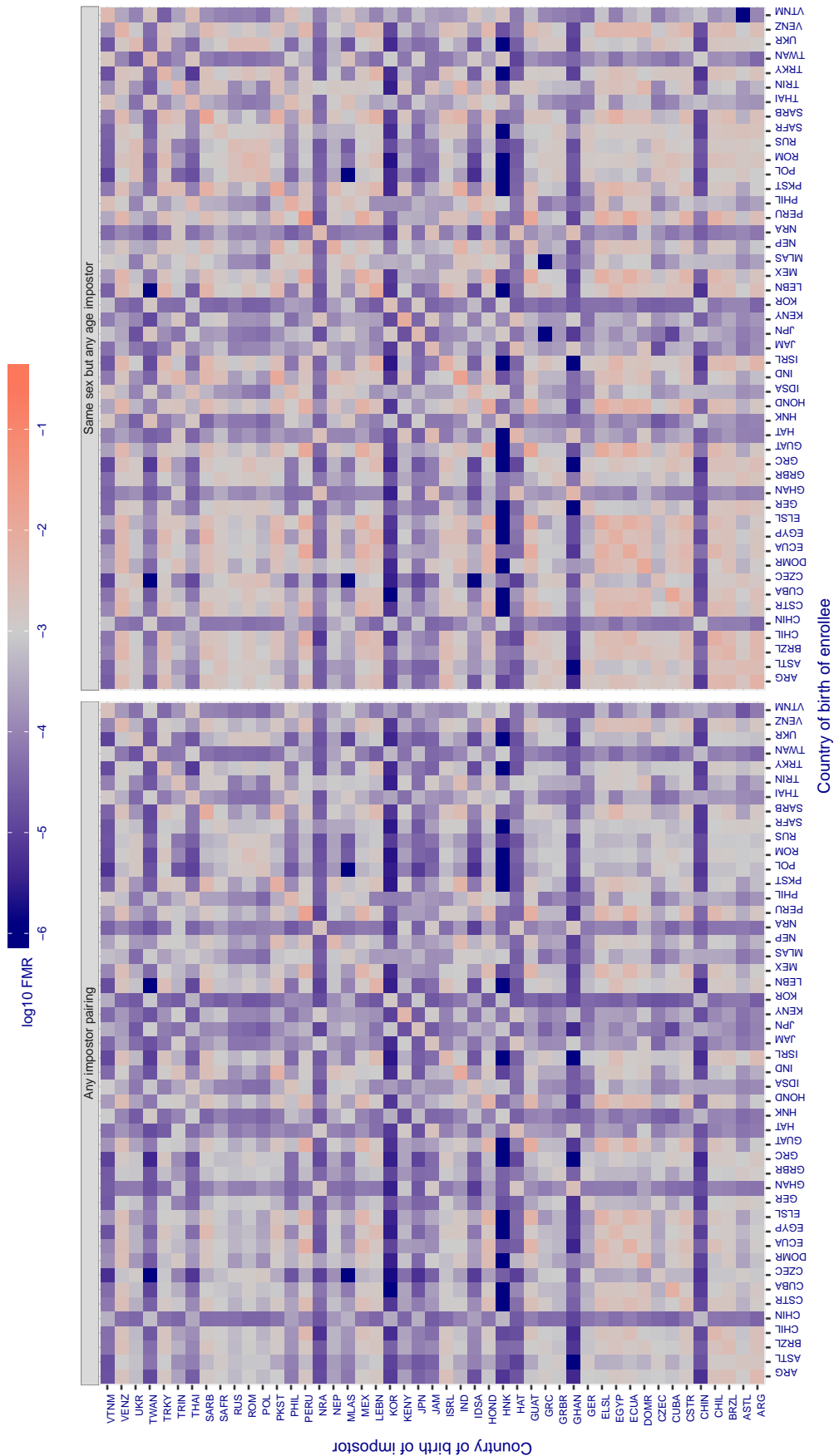


Figure 122: For algorithm yitu-000 operating on visa images, the heatmap shows false match rates observed over impostor comparisons of faces from different individuals who were born in the given country pair. False matches are counted against a recognition threshold fixed globally to give the target FMR in the plot title, computed over all $O(10^{10})$ impostor comparisons. If text appears in each box it give the same quantity as that coded by the color. Grey indicates FMR is at the intended FMR target level. Light red colors present a security vulnerability to, for example, a passport gate. Each +1 increase in $\log_{10} FMR$ corresponds to a factor of 10 increase in FMR. The matrix is not quite symmetric because images in the enrollment and verification sets are different.

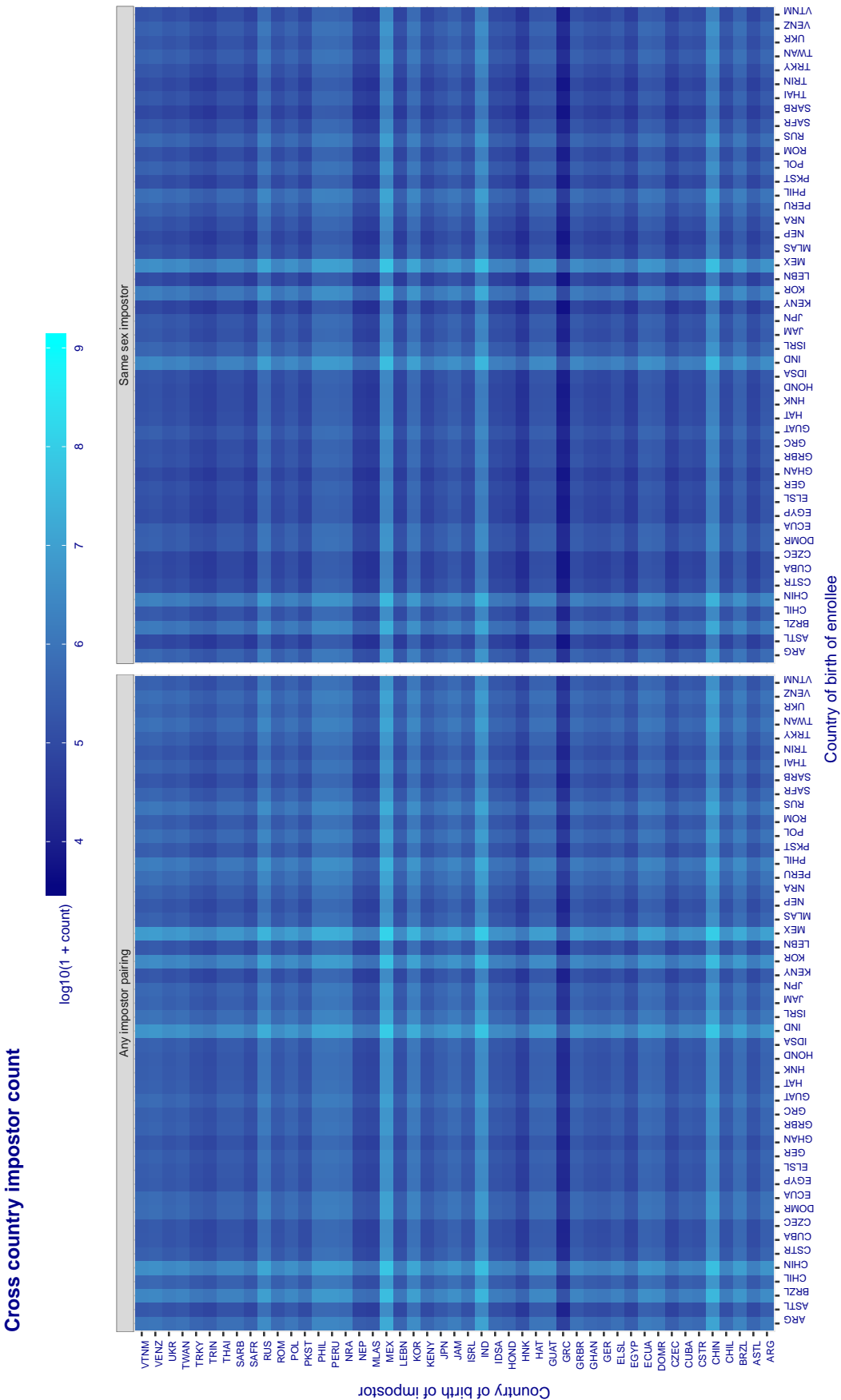


Figure 123: For visa images, the heatmap shows the count of impostor comparisons of faces from different individuals who were born in the given country pair.

5.6.2 Effect of age on impostors

Background: This section shows the effect of age on the impostor distribution. The ideal behaviour is that the age of the enrollee and the impostor would not affect impostor scores. This would support FMR stability over sub-populations.

Goals:

- ▷ To show the effect of relative ages of the impostor and enrollee on false match rates.
- ▷ To determine whether some algorithms have better impostor distribution stability.

Methods:

- ▷ Define 14 age group bins, spanning 0 to over 100 years old.
- ▷ Compute FMR over all impostor comparisons for which the subjects in the enrollee and impostor images have ages in two bins.
- ▷ Compute FMR over all impostor comparisons for which the subjects are additionally of the same sex, and born in the same geographic region.

Results:

The notable aspects are:

- ▷ Diagonal dominance: Impostors are more likely to be matched against their same age group.
- ▷ Same sex and same region impostors are more successful. On the diagonal, an impostor is more likely to succeed by posing as someone of the same sex. If $\Delta \log_{10} \text{FMR} = 0.2$, then same-sex same-region FMR exceeds the all-pairs FMR by factor of $10^{0.2} = 1.6$.
- ▷ Young children impostors give elevated FMR against young children. Older adult impostor give elevated FMR against older adults. These effects are quite large, for example if $\Delta \log_{10} \text{FMR} = 1.0$ larger than a 32 year old, then these groups have higher FMR by a factor of $10^1 = 10$. This would imply an FMR above 0.01 for a nominal (global) FMR = 0.001.
- ▷ Algorithms vary.
- ▷ We computed the same quantities for a global FMR = 0.0001. The effects are similar.

Note the calculations in this section include impostors paired across all countries of birth.

Cross age FMR at threshold $T = 2.899$ for algorithm 3divi_001, giving $FMR(T) = 0.0001$ globally.

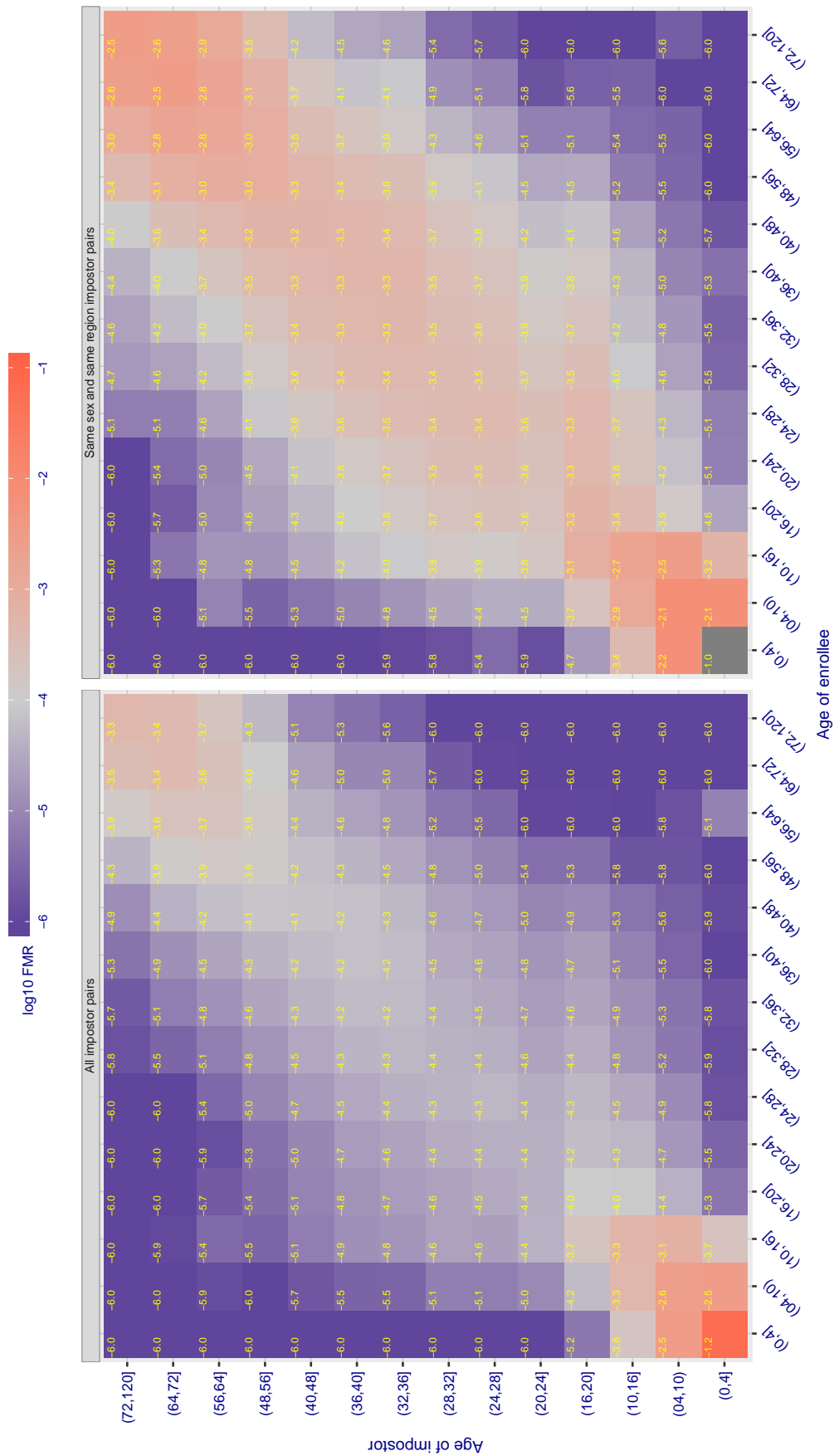


Figure 124: For algorithm 3divi-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 2.899$ for algorithm 3divi_002, giving $FMR(T) = 0.0001$ globally.

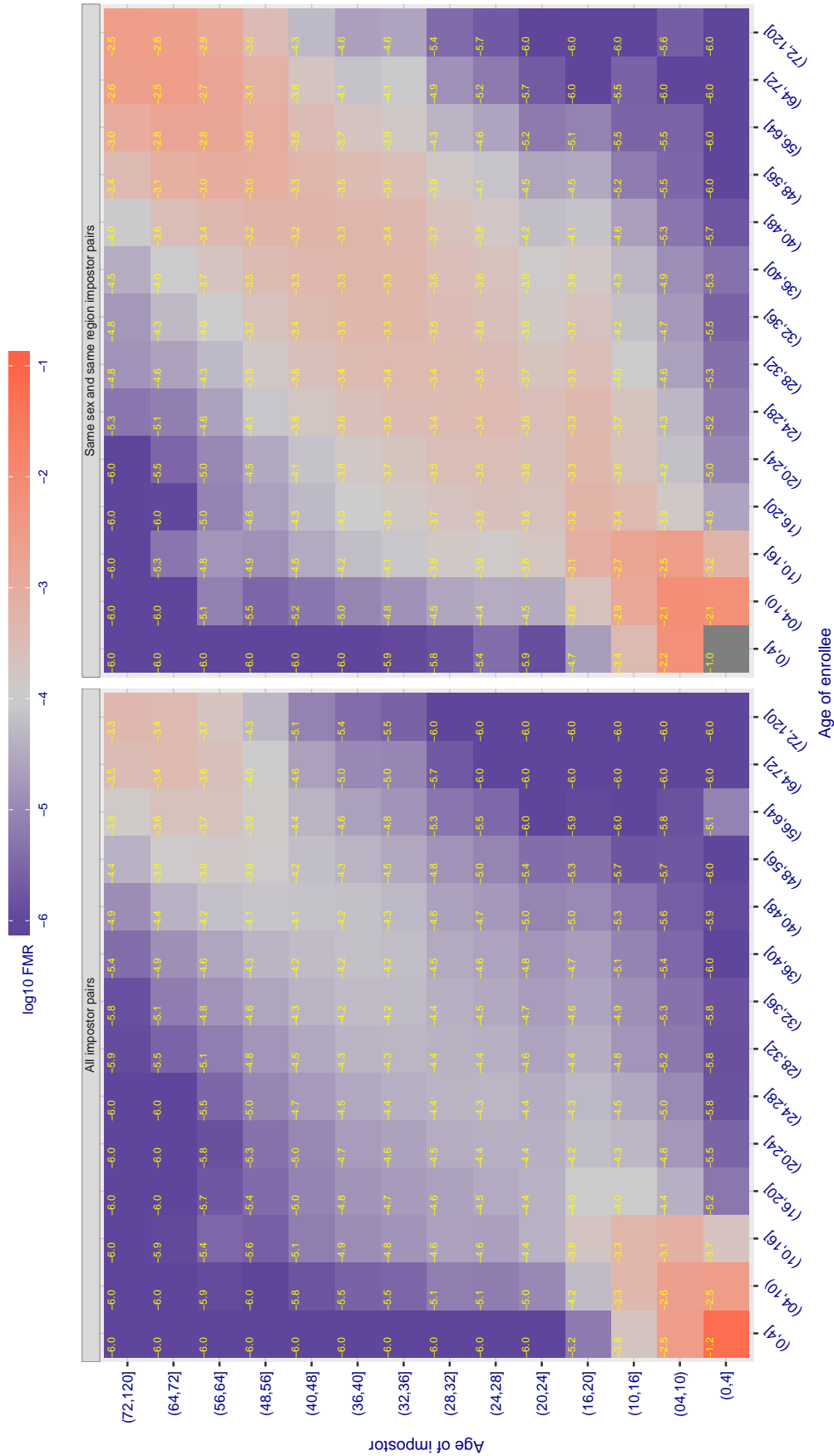


Figure 125: For algorithm 3divi-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 4.029$ for algorithm aware_000, giving $FMR(T) = 0.0001$ globally.

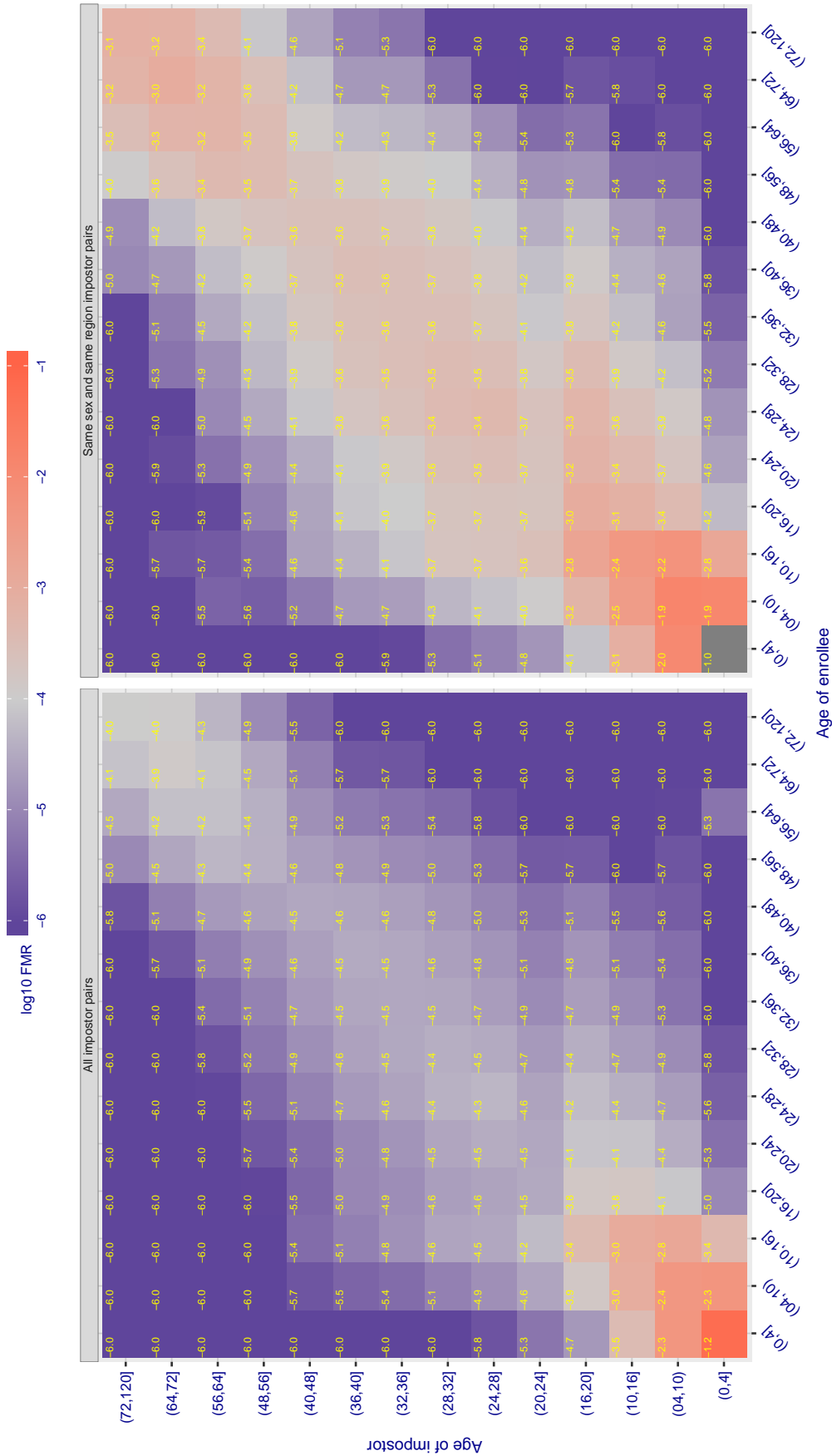


Figure 126: For algorithm aware-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 4.029$ for algorithm aware_001, giving $FMR(T) = 0.0001$ globally.

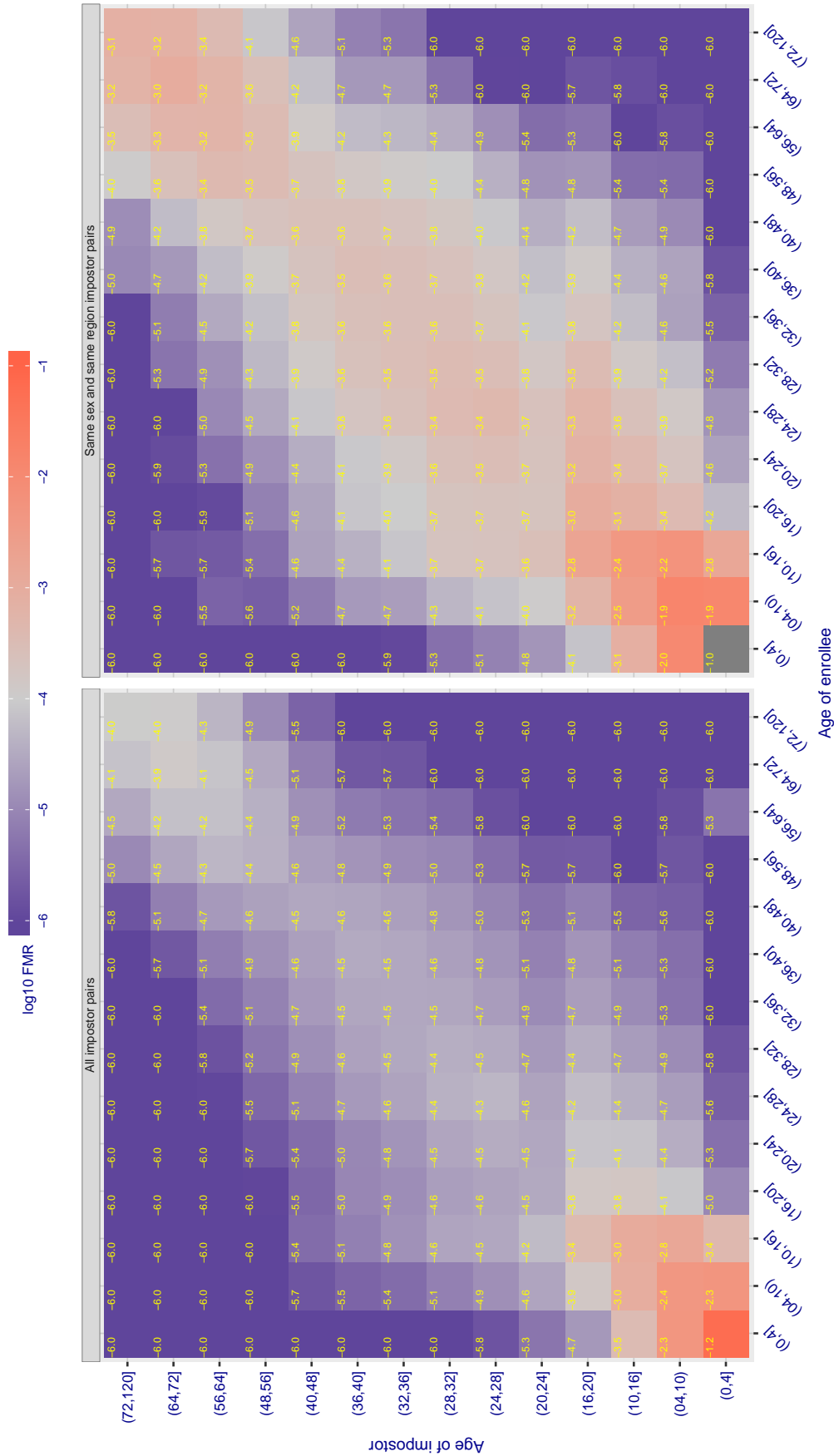


Figure 127: For algorithm aware-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.919$ for algorithm ayonix_000, giving $FMR(T) = 0.0001$ globally.

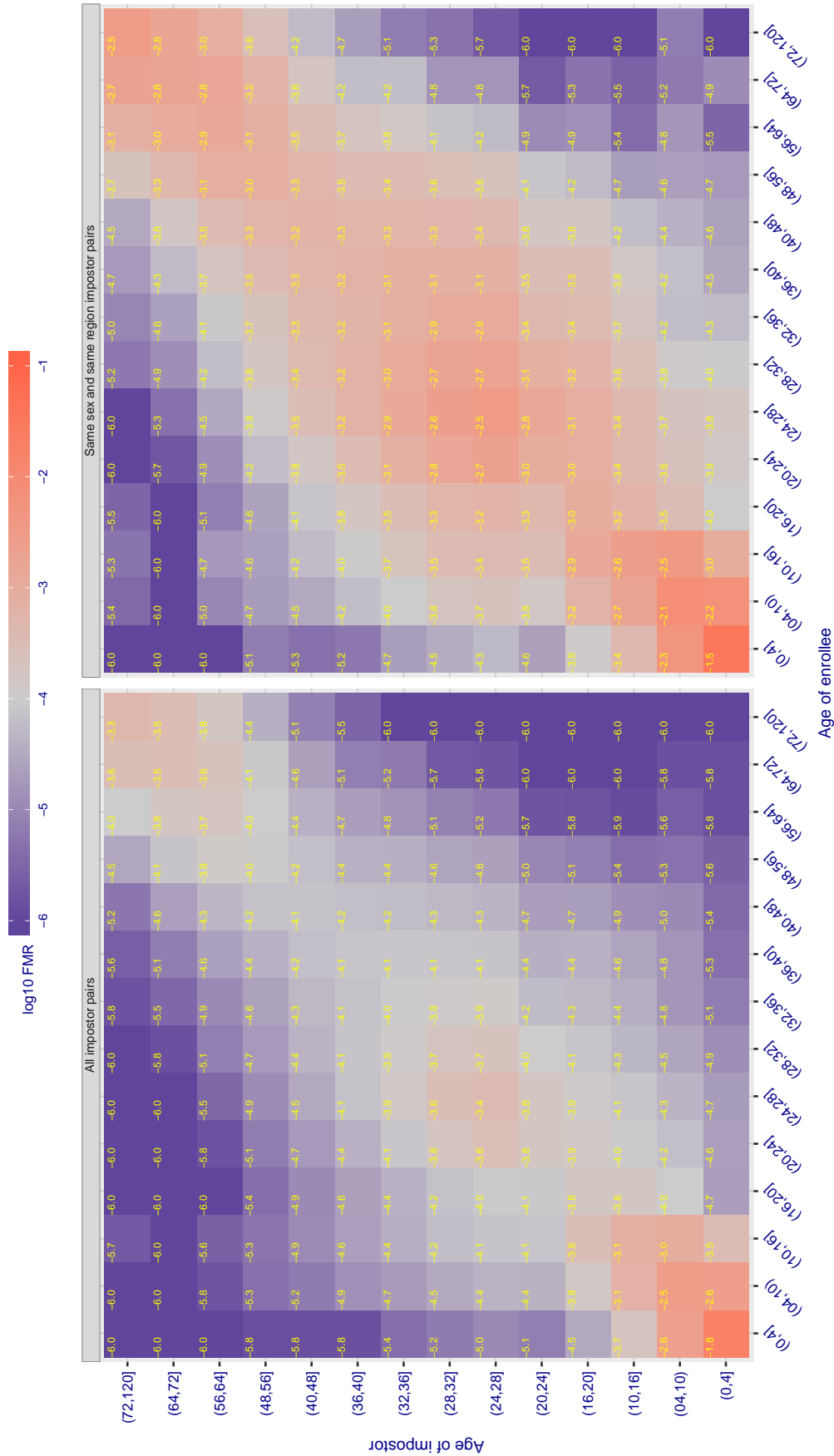


Figure 128: For algorithm ayonix-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.681$ for algorithm camvi_001, giving $FMR(T) = 0.0001$ globally.

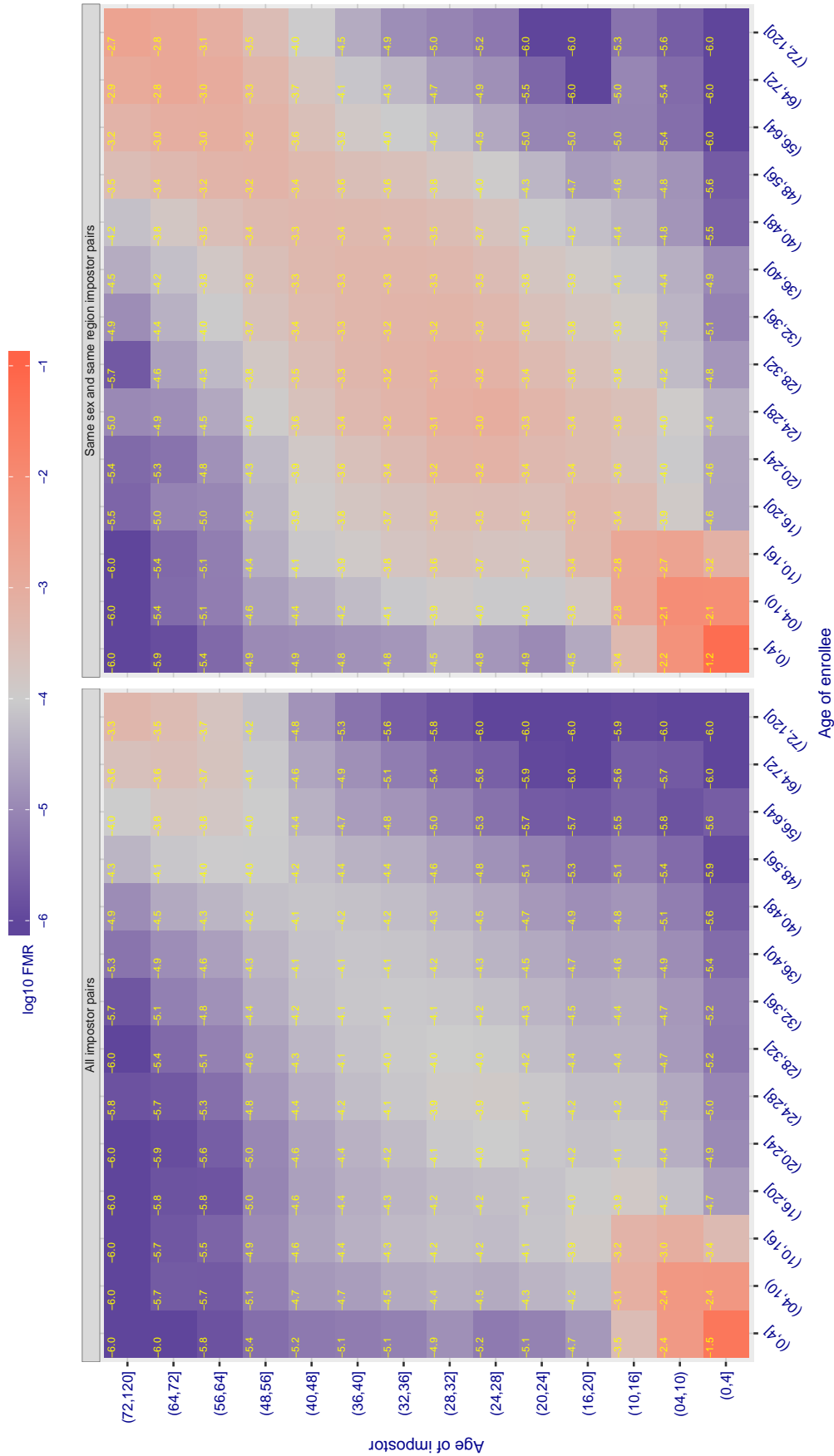


Figure 129: For algorithm camvi-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 3564.000$ for algorithm cogent_000, giving $FMR(T) = 0.0001$ globally.

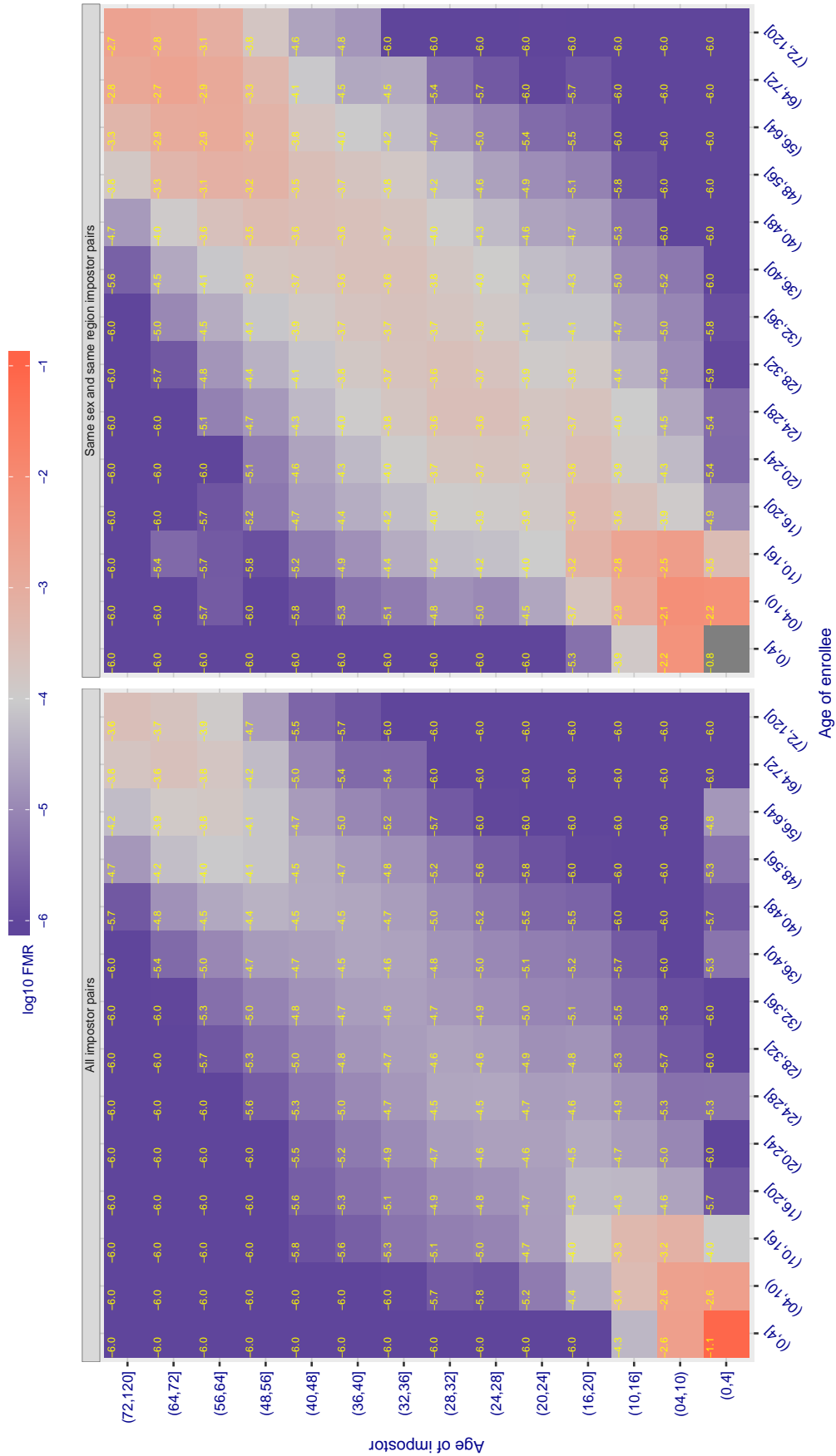


Figure 130: For algorithm cogent-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.762$ for algorithm cyberextruder_001, giving $FMR(T) = 0.0001$ globally.

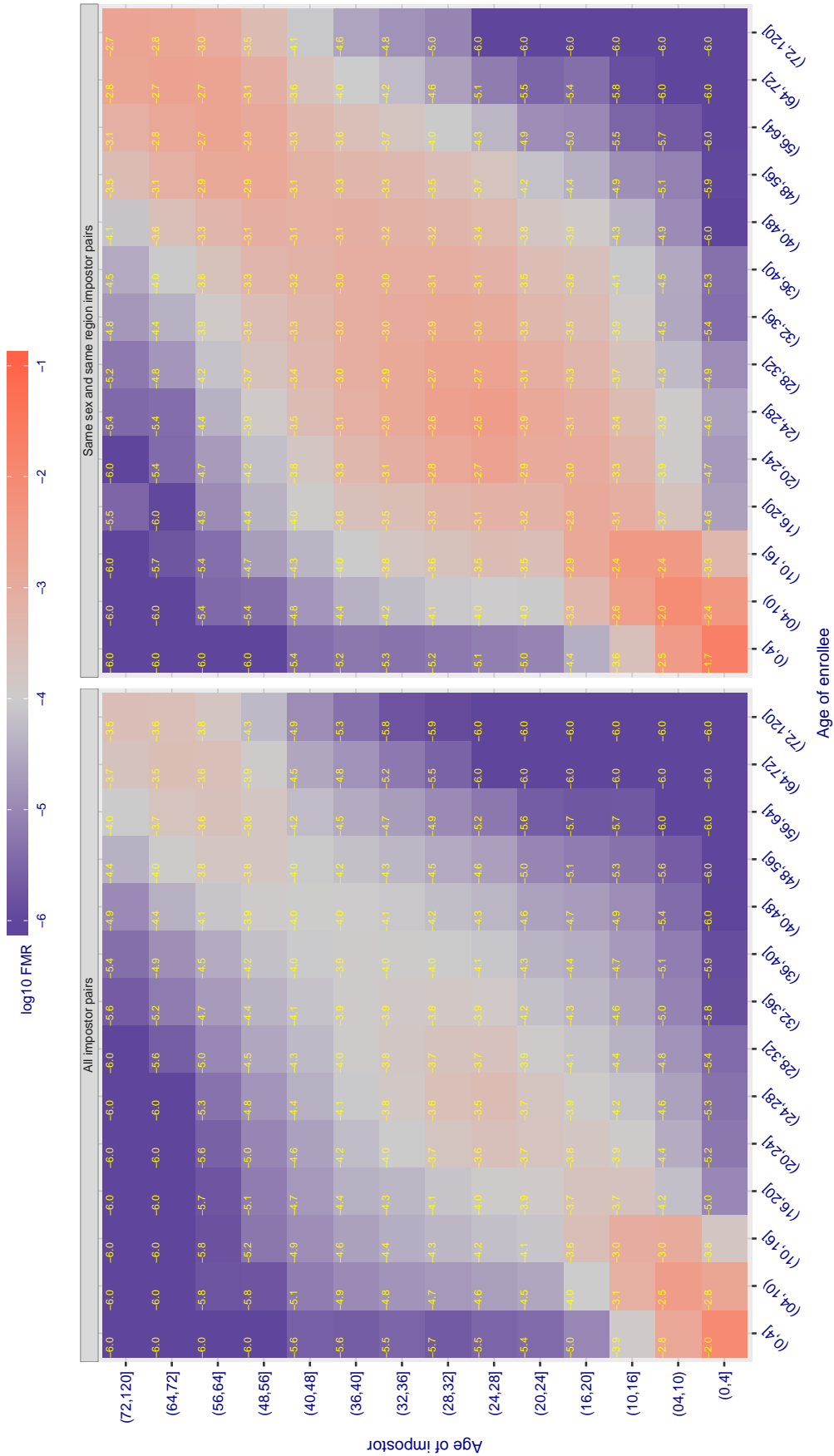


Figure 131: For algorithm cyberextruder-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 84.718$ for algorithm dermalog_003, giving $FMR(T) = 0.0001$ globally.

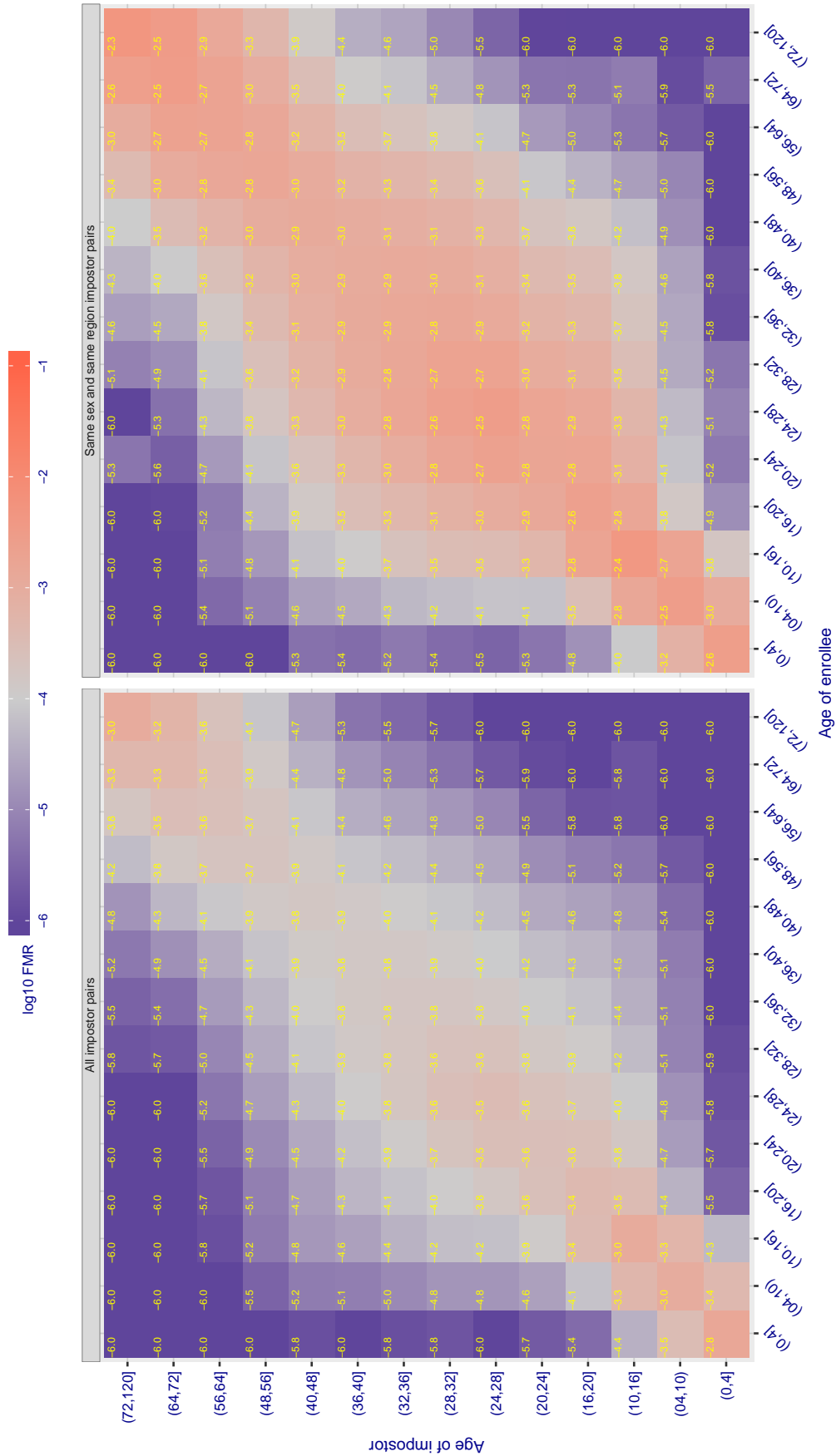


Figure 132: For algorithm dermalog-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 81.959$ for algorithm dermalog_004, giving $FMR(T) = 0.0001$ globally.

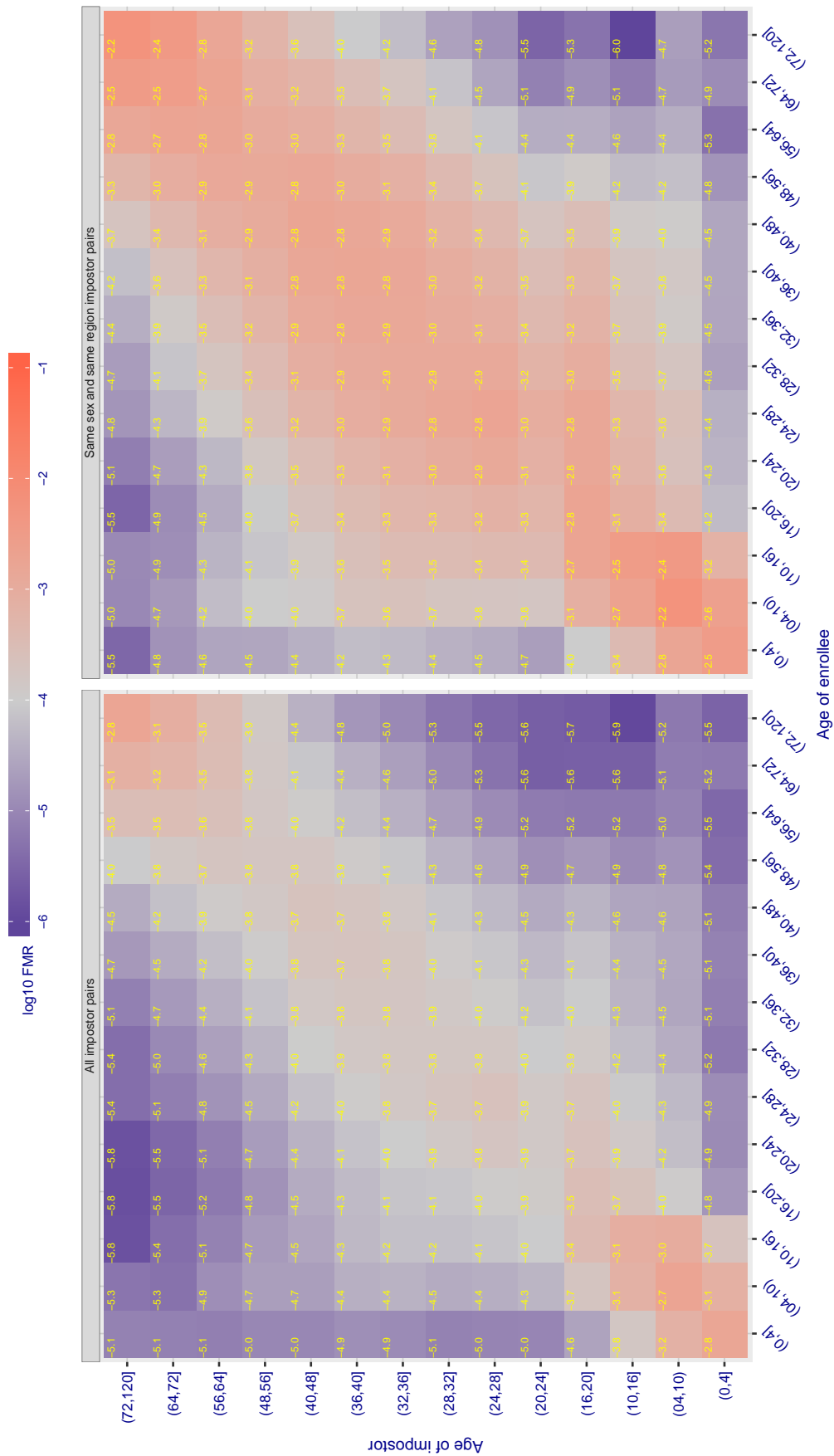


Figure 133: For algorithm dermalog-004 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.646$ for algorithm digitalbarriers_000, giving $FMR(T) = 0.0001$ globally.

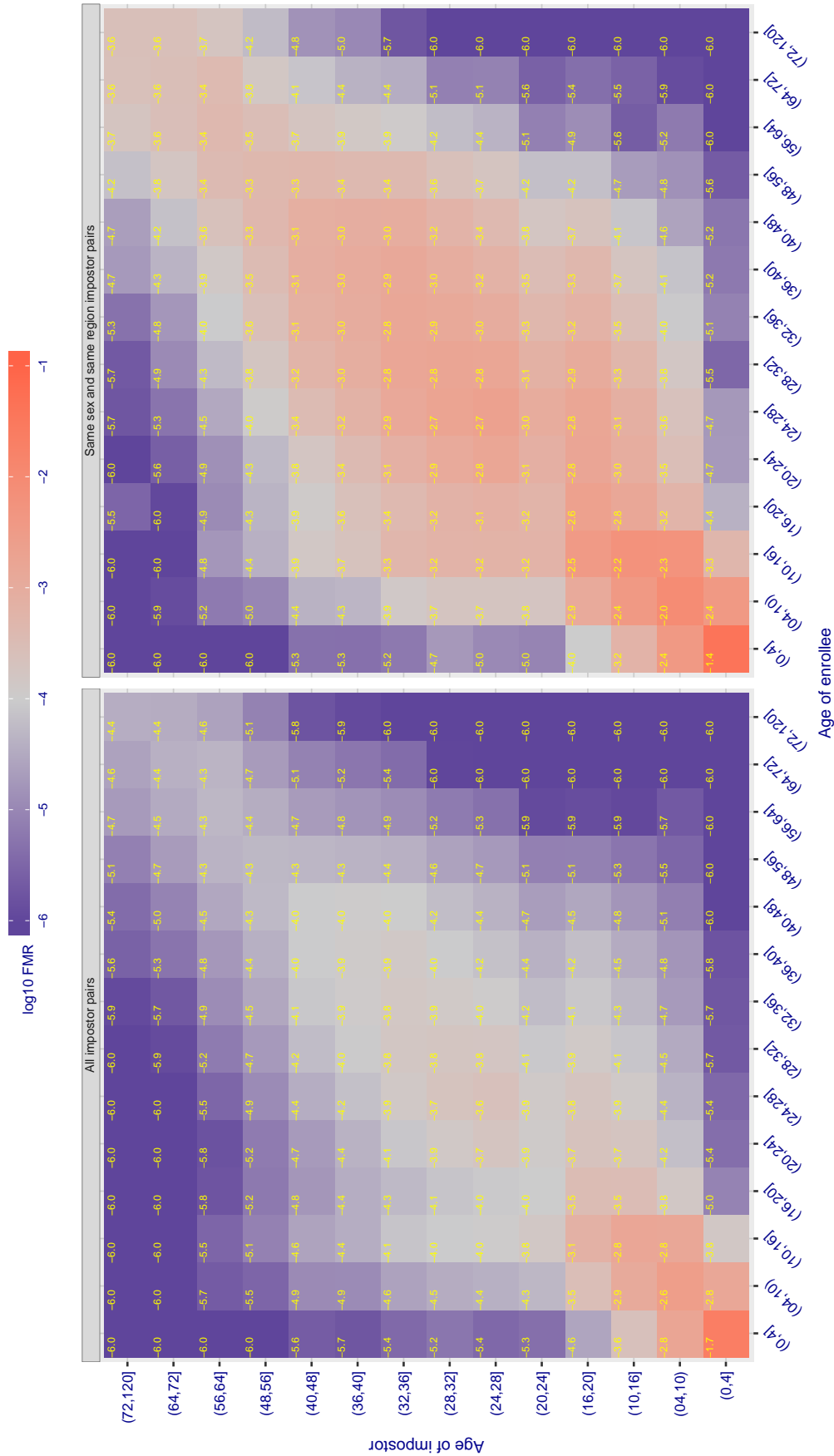


Figure 134: For algorithm digitalbarriers-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.700$ for algorithm digitalbarriers_001, giving $FMR(T) = 0.0001$ globally.

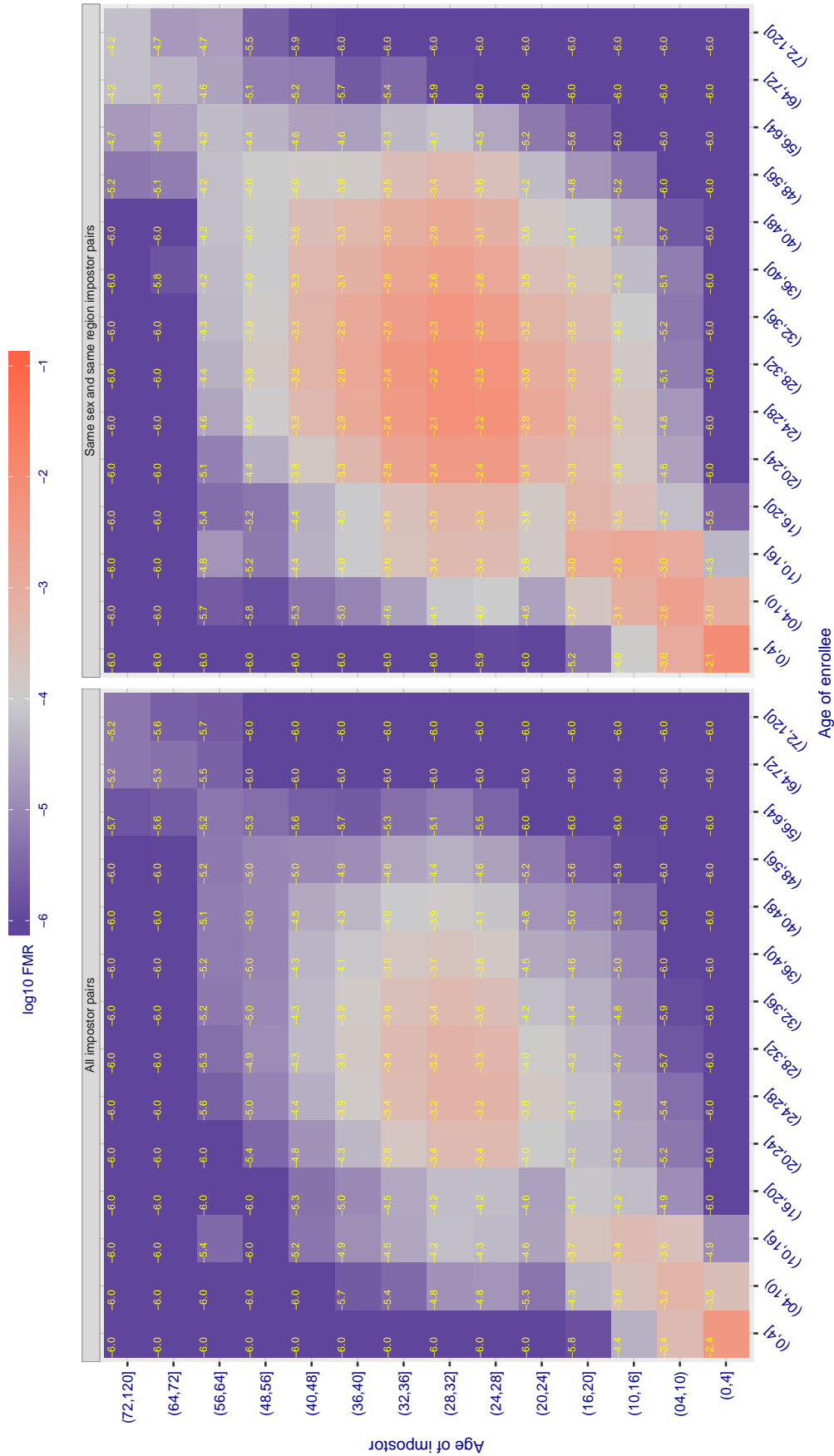


Figure 135: For algorithm digitalbarriers-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.798$ for algorithm fdu_000 , giving $\text{FMR}(T) = 0.0001$ globally.

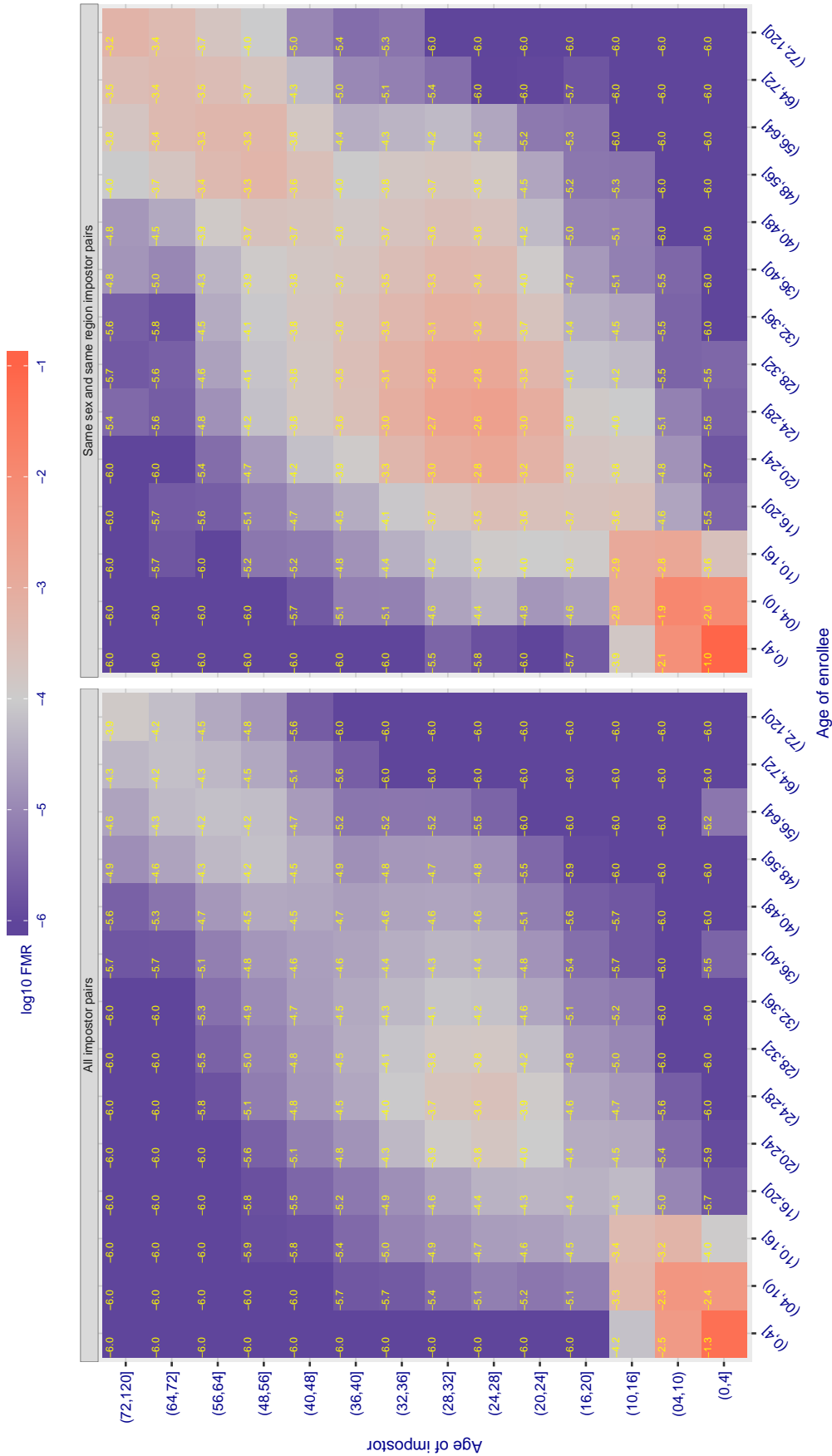


Figure 136: For algorithm fdu_000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $\text{FMR} = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.850$ for algorithm fdu_001 , giving $\text{FMR}(T) = 0.0001$ globally.

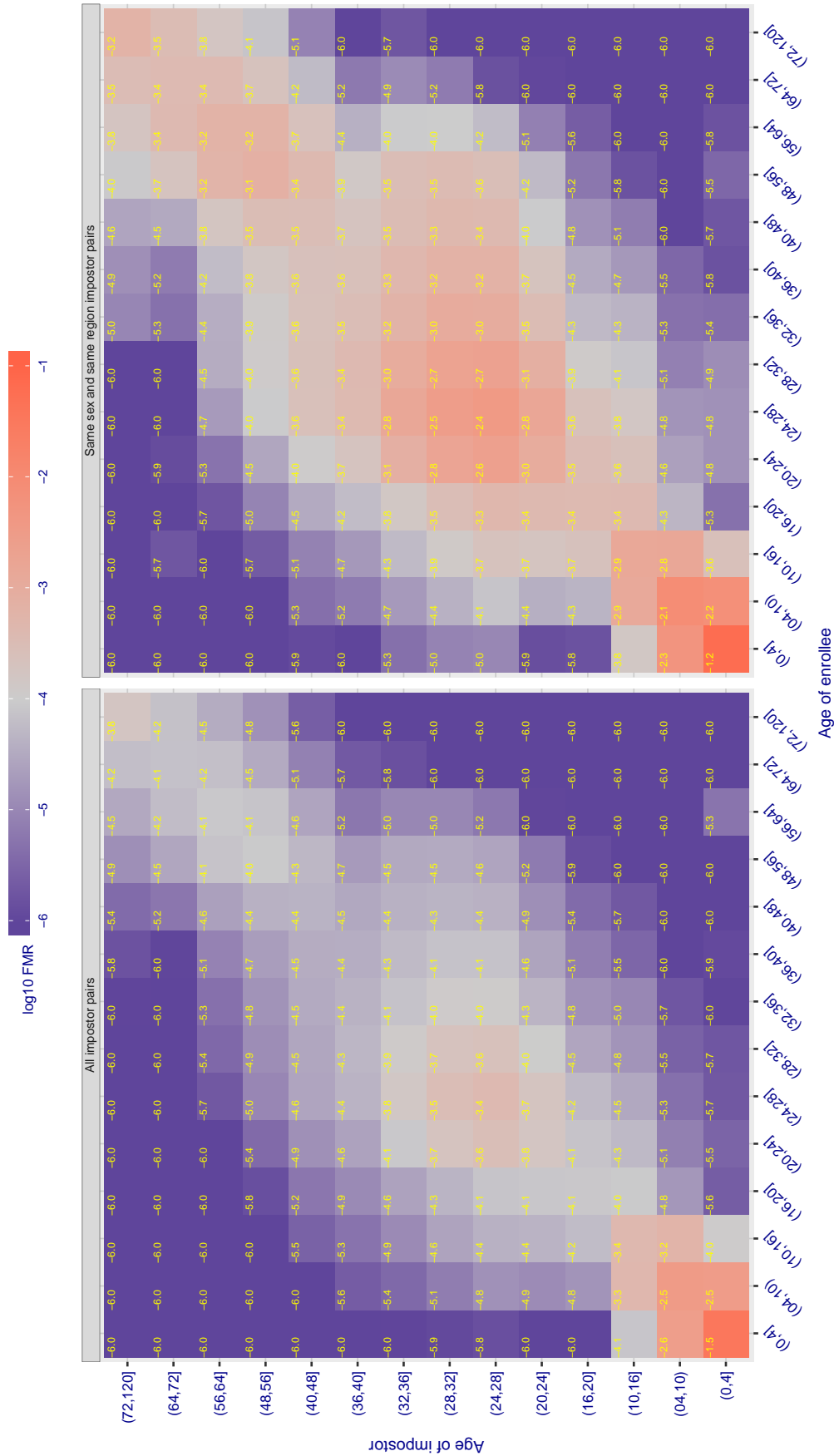


Figure 137: For algorithm fdu_001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $\text{FMR} = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 2611.000$ for algorithm id3_001, giving $FMR(T) = 0.0001$ globally.

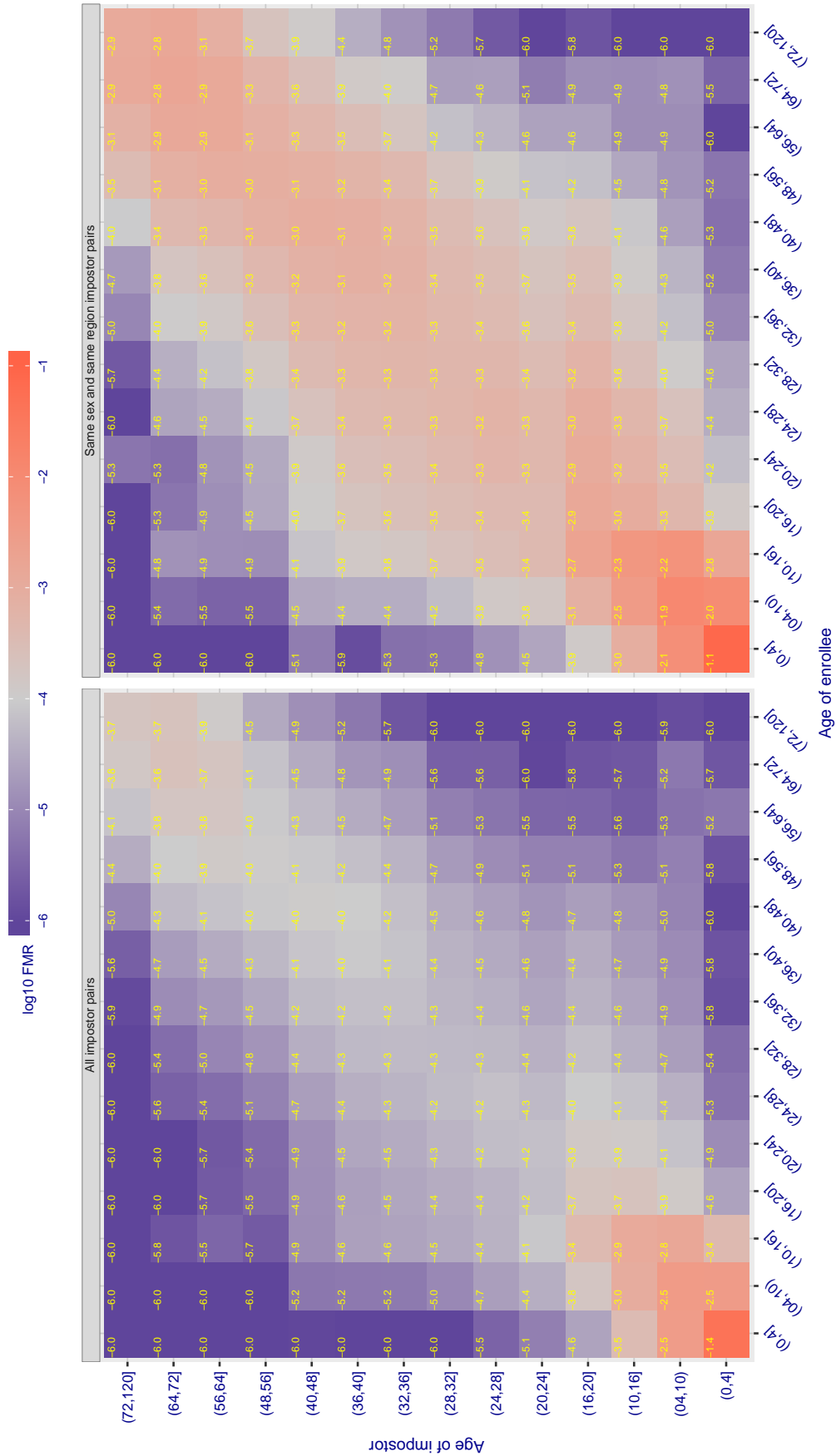


Figure 138: For algorithm id3-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 2649.000$ for algorithm id3_002, giving $FMR(T) = 0.0001$ globally.

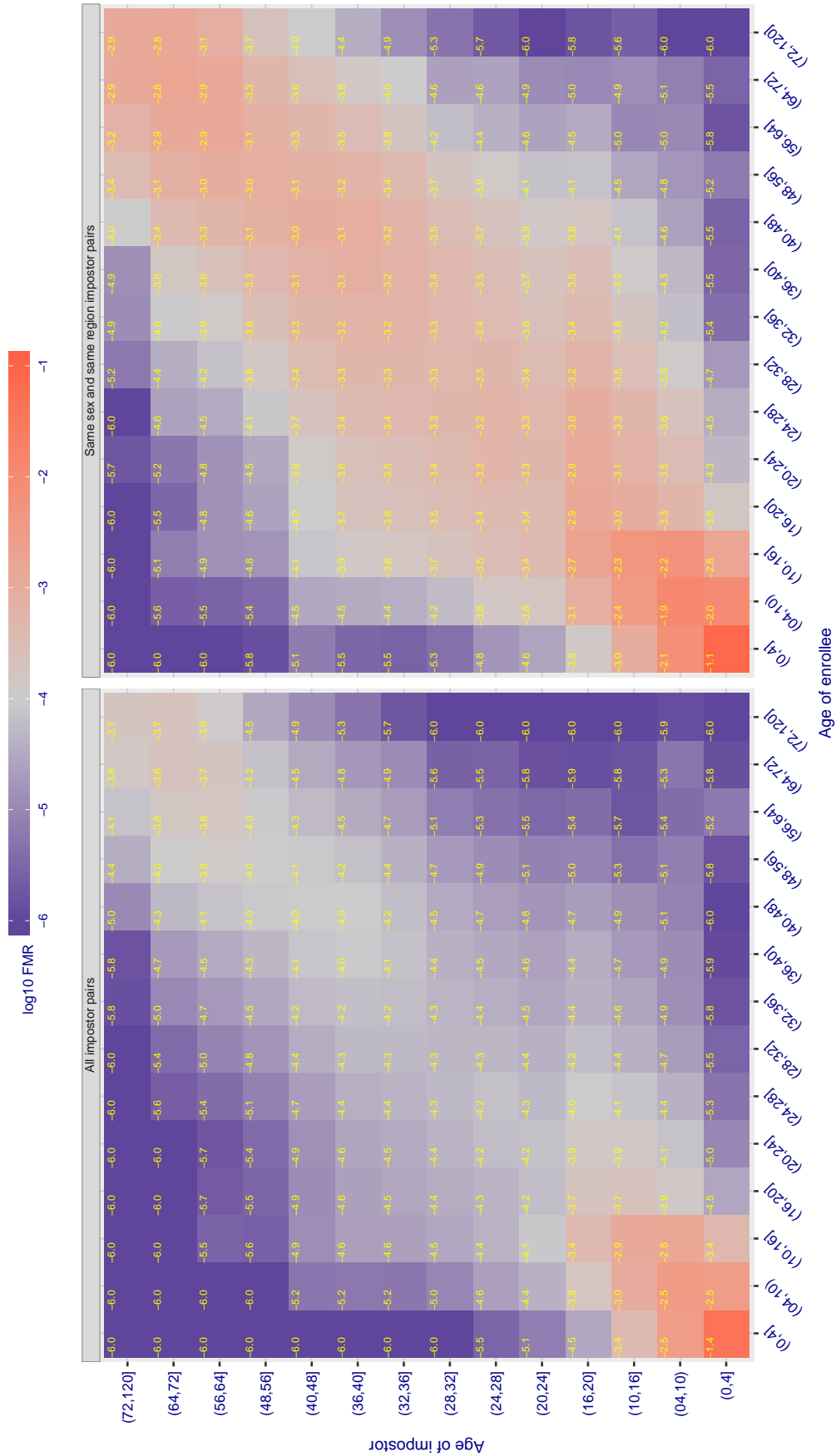


Figure 139: For algorithm id3-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.0001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 58.258$ for algorithm innovatrics_000, giving $FMR(T) = 0.0001$ globally.

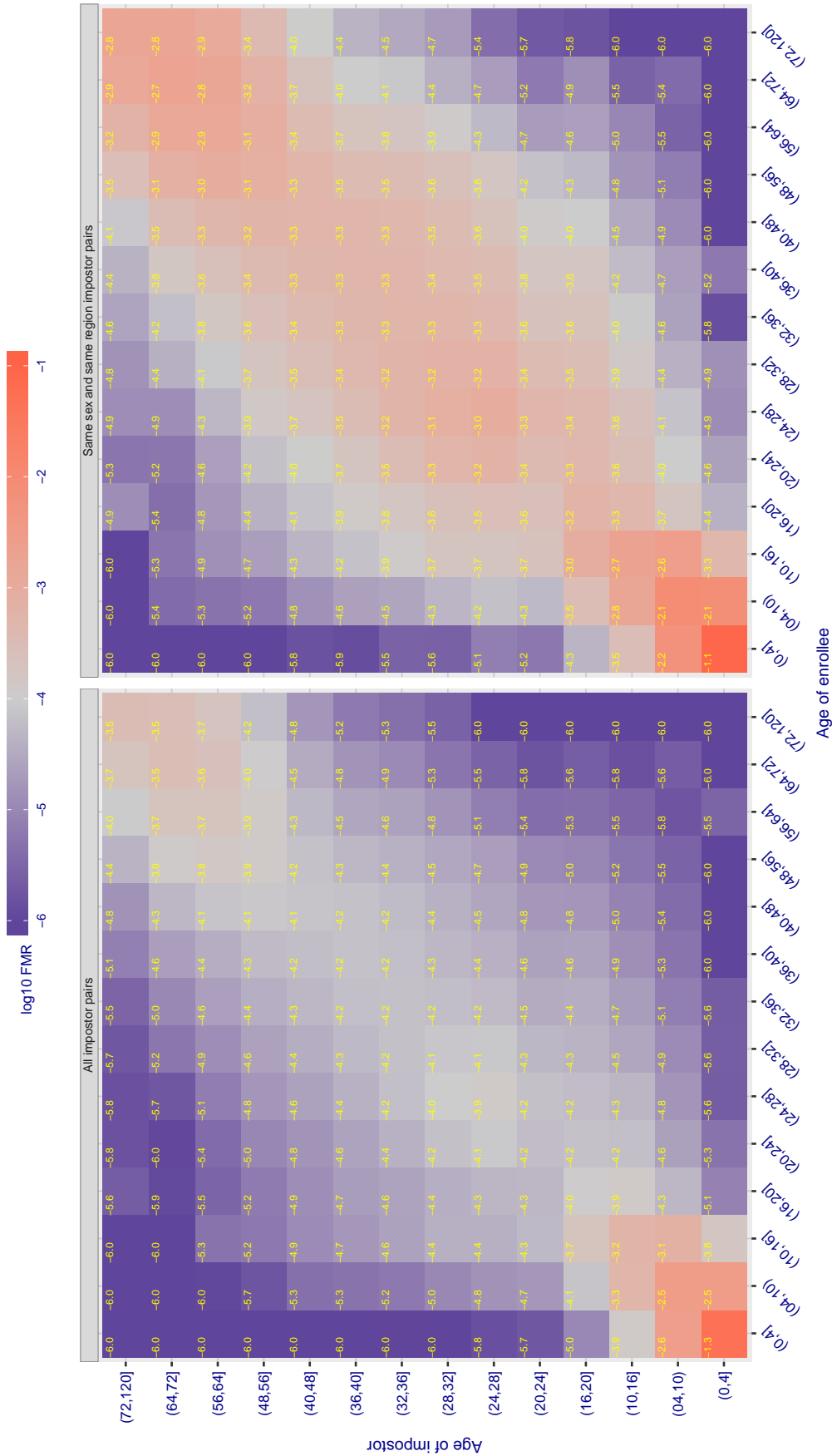


Figure 140: For algorithm innovatrics-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 54.156$ for algorithm innovatrics_001, giving $FMR(T) = 0.0001$ globally.

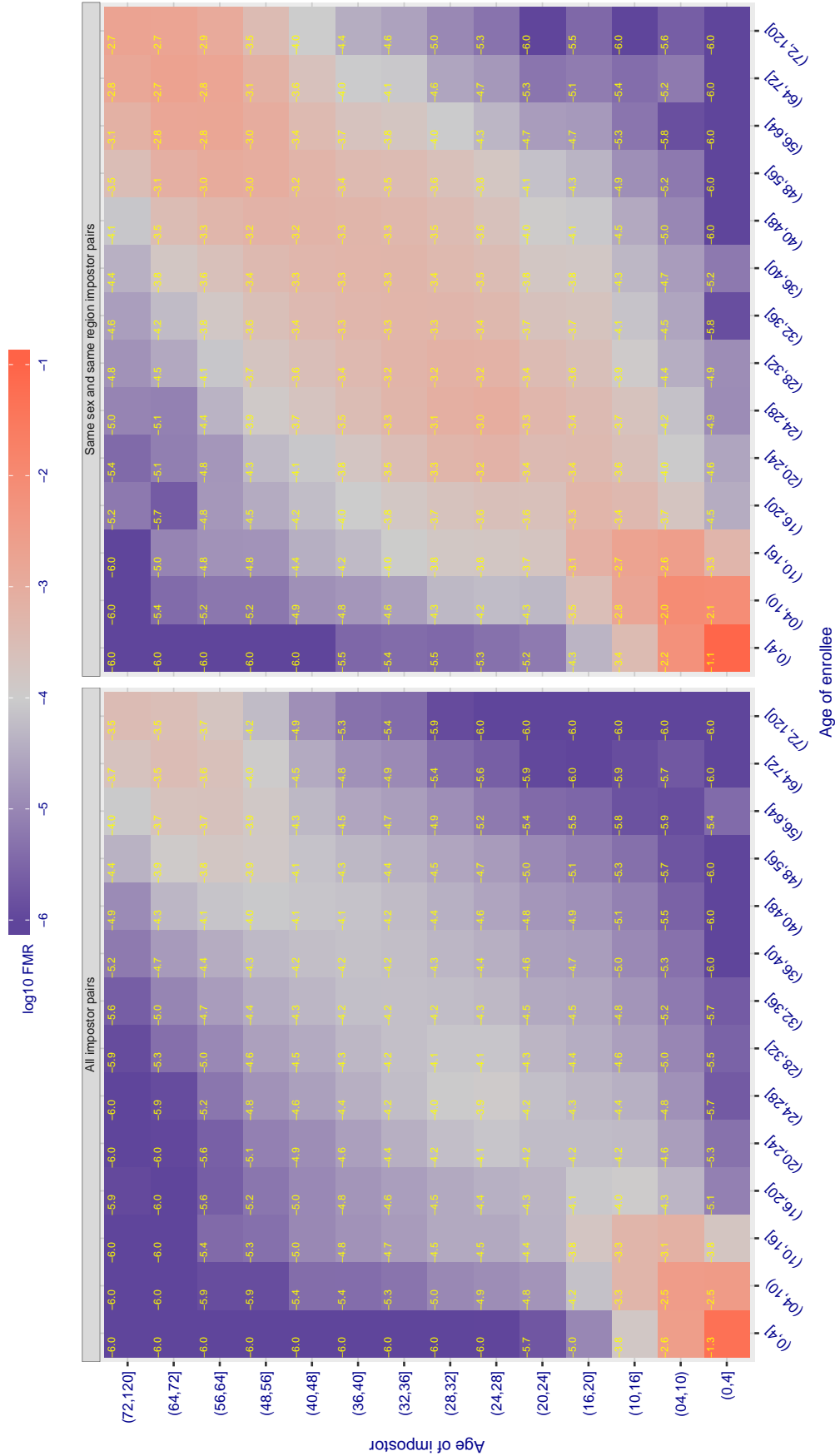


Figure 141: For algorithm innovatrics-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 49.664$ for algorithm intellivision_001, giving $FMR(T) = 0.0001$ globally.

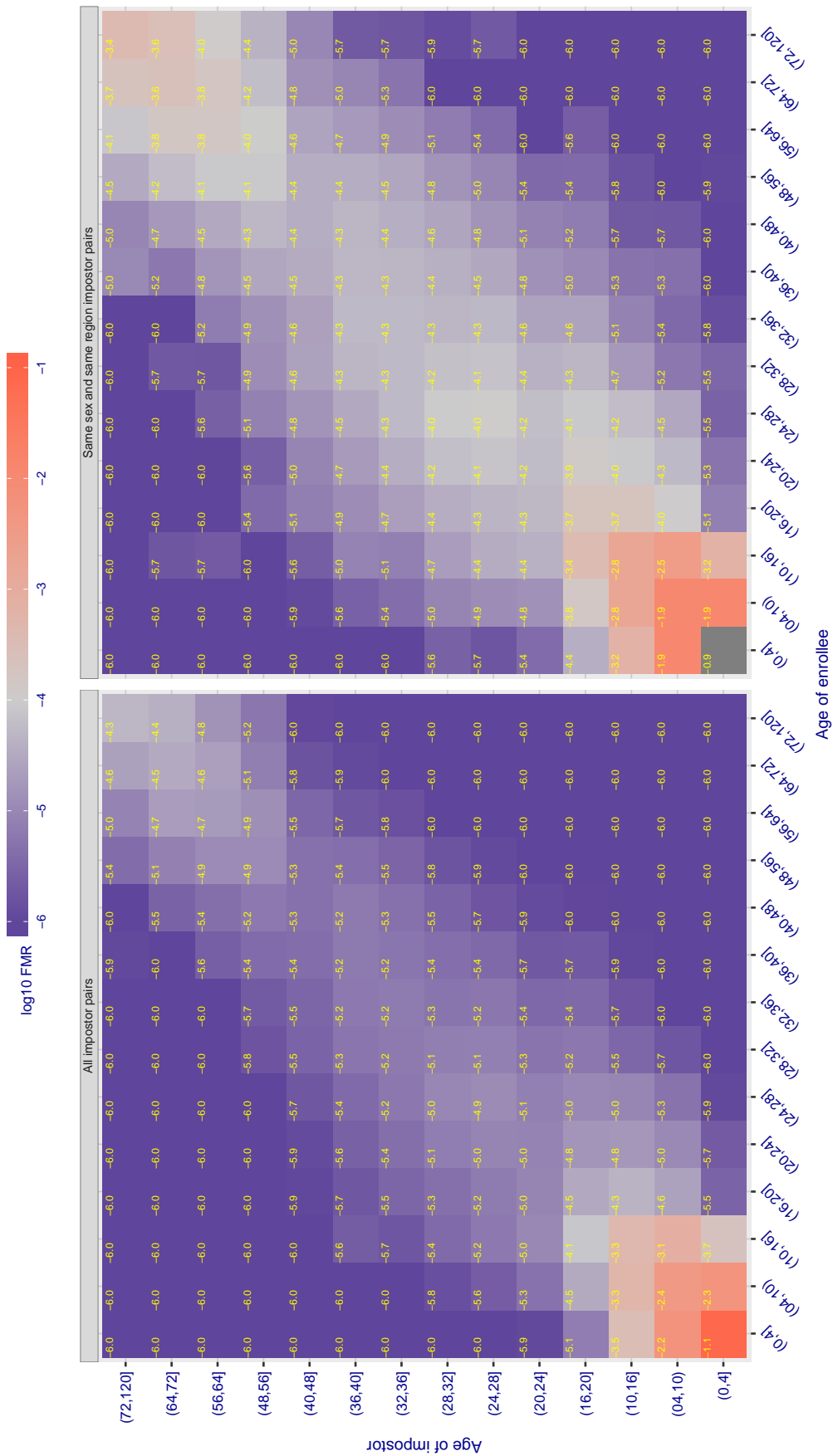


Figure 142: For algorithm intellivision-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 23.498$ for algorithm isityou_000, giving $FMR(T) = 0.0001$ globally.

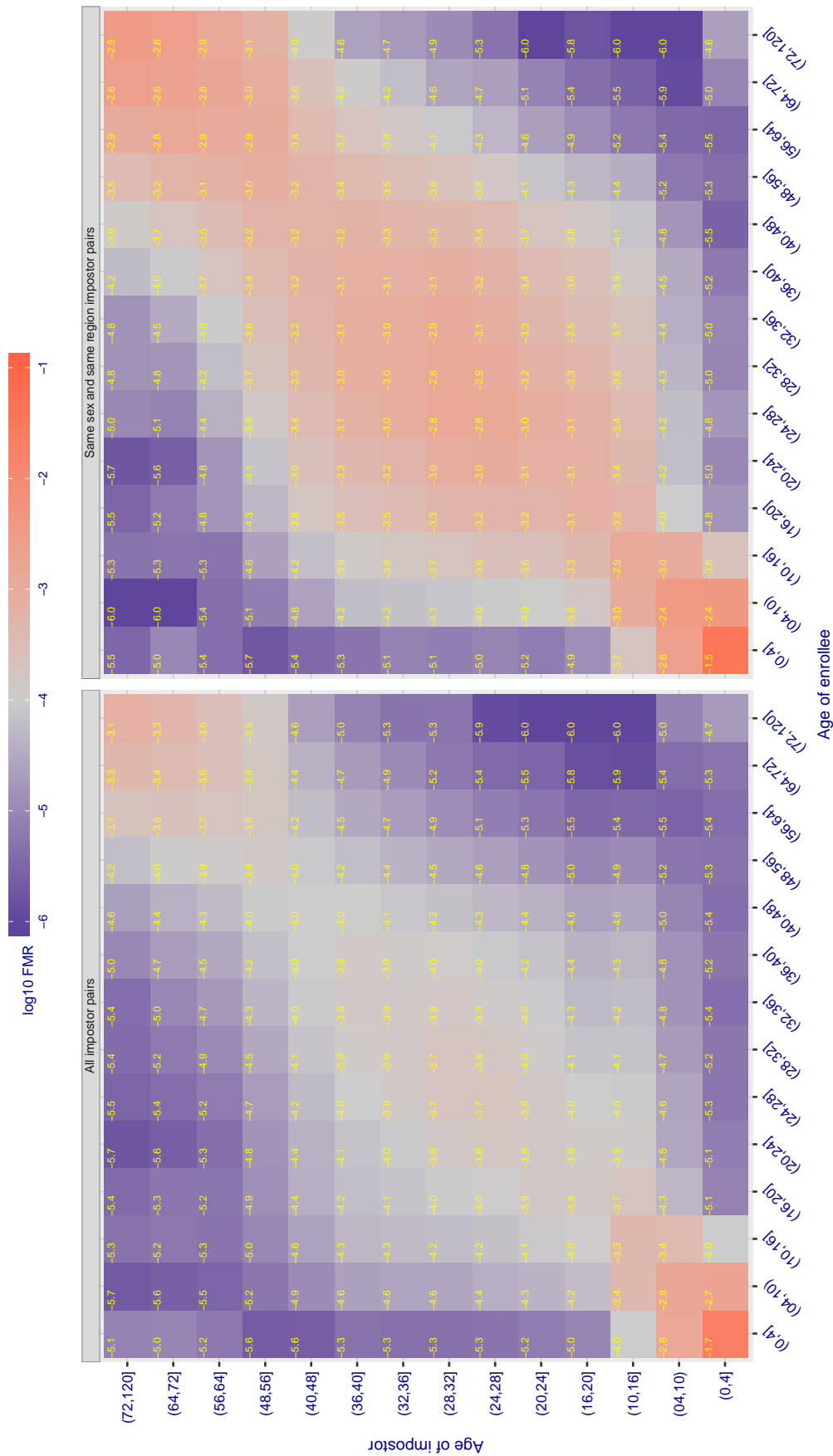


Figure 143: For algorithm isityou-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.782$ for algorithm isystems_000, giving $FMR(T) = 0.0001$ globally.

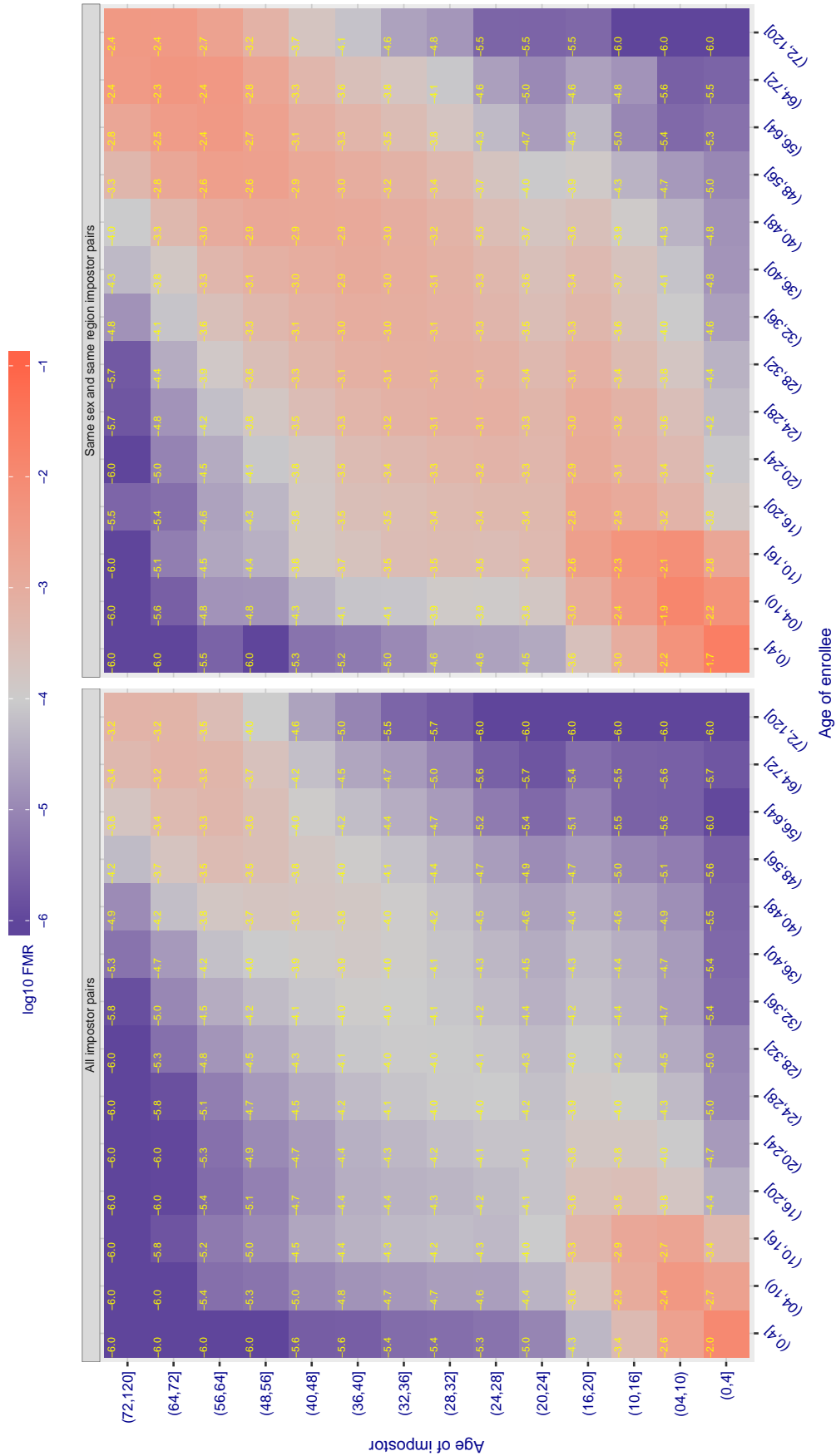


Figure 144: For algorithm isystems-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 998.683$ for algorithm itmo_002, giving $FMR(T) = 0.0001$ globally.

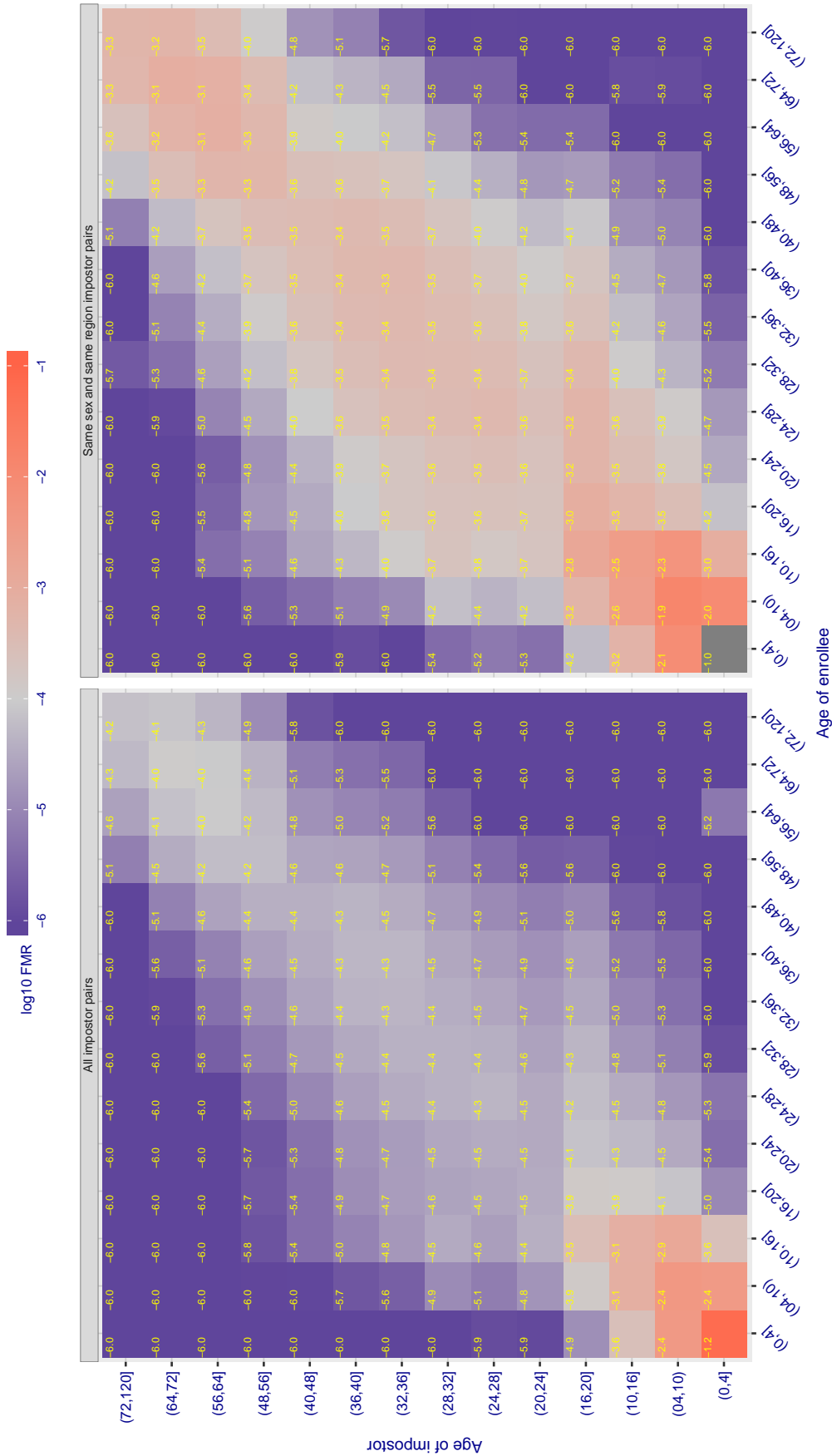


Figure 145: For algorithm itmo-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 3846.708$ for algorithm morpho_000, giving $FMR(T) = 0.0001$ globally.

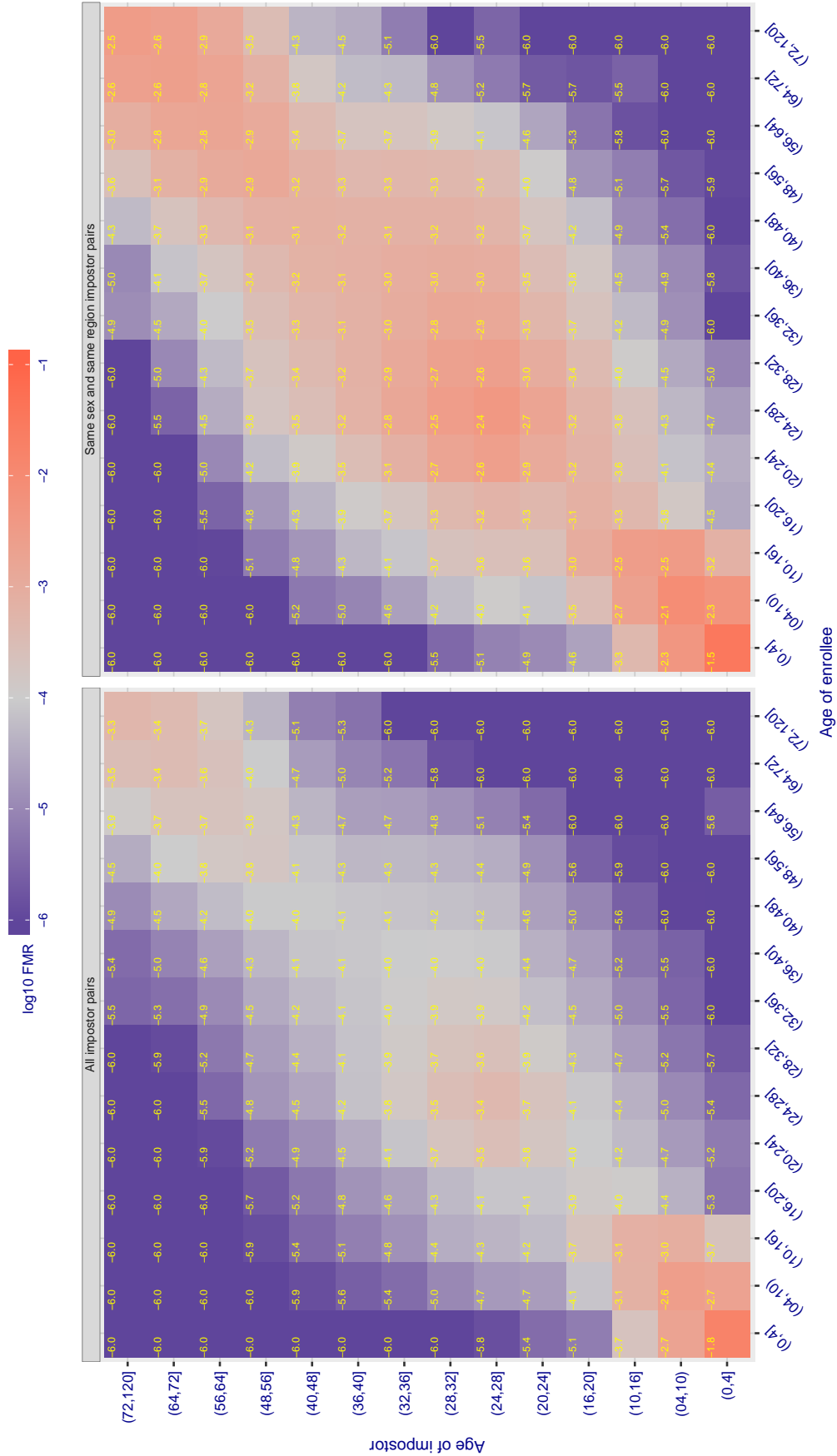


Figure 146: For algorithm morpho-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 3801.880$ for algorithm morpho_002, giving $FMR(T) = 0.0001$ globally.

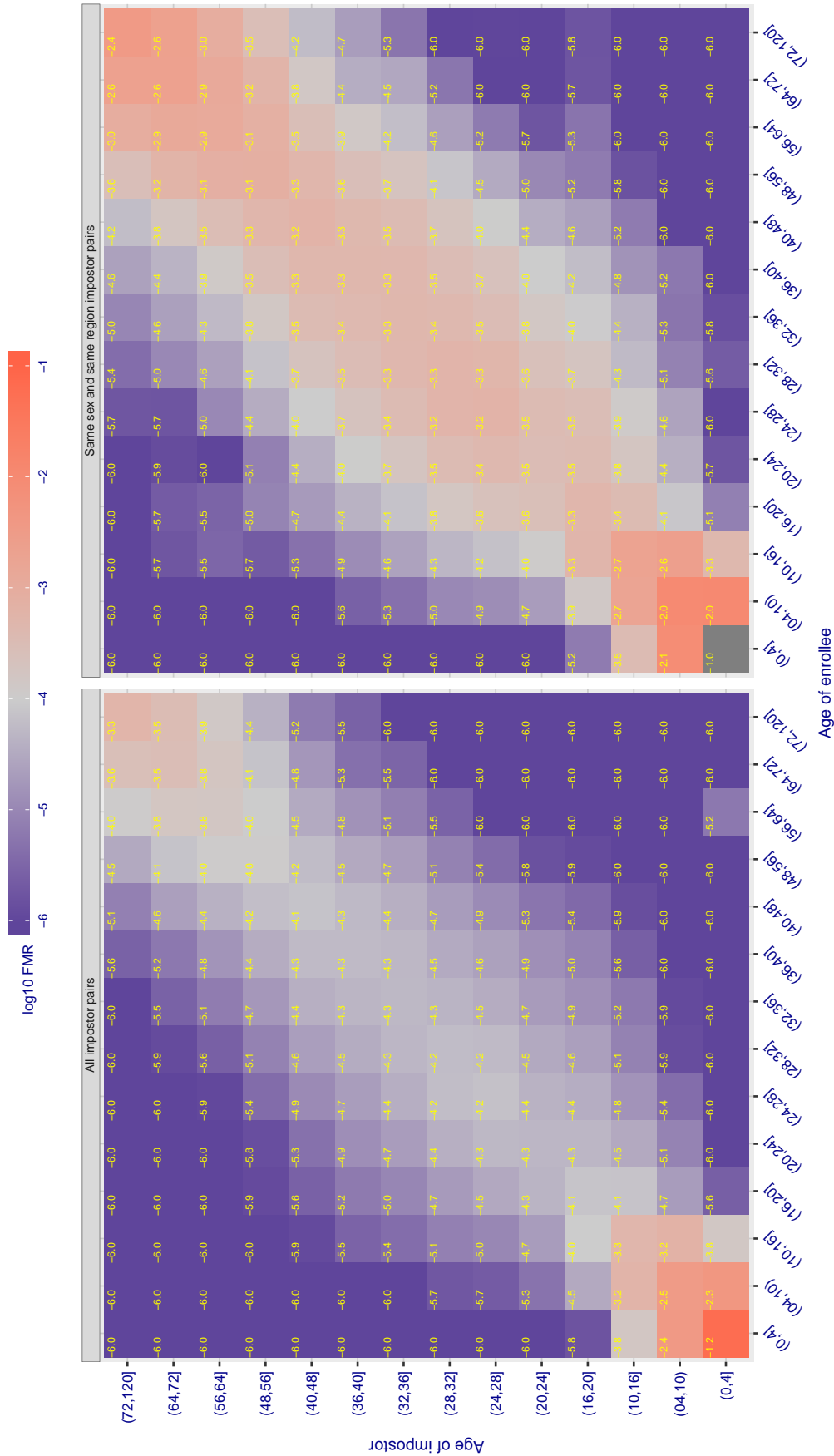


Figure 147: For algorithm morpho-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 45.600$ for algorithm neurotechnology_001, giving $FMR(T) = 0.0001$ globally.

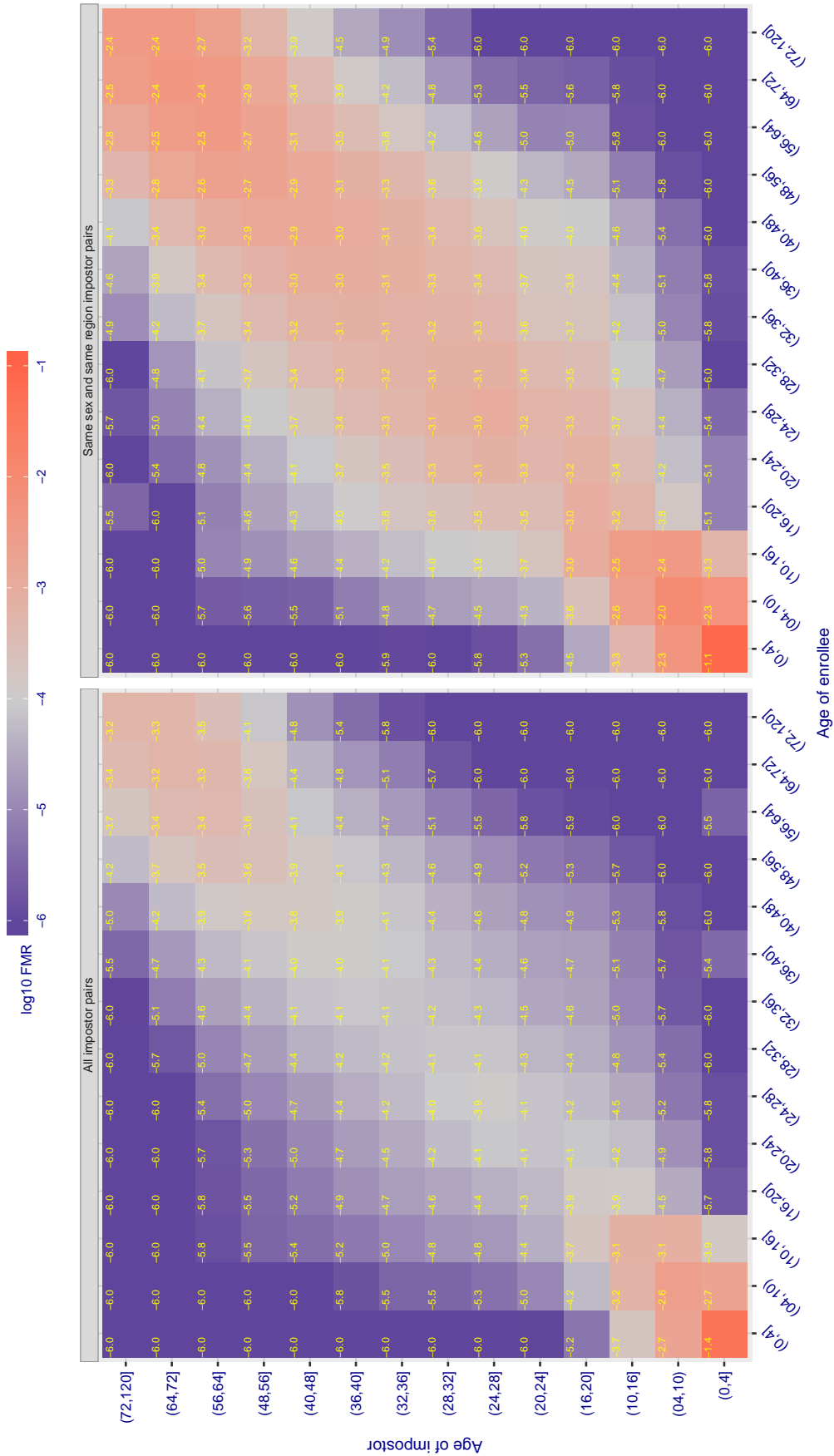


Figure 148: For algorithm neurotechnology-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 43.590$ for algorithm neurotechnology_002, giving $FMR(T) = 0.0001$ globally.

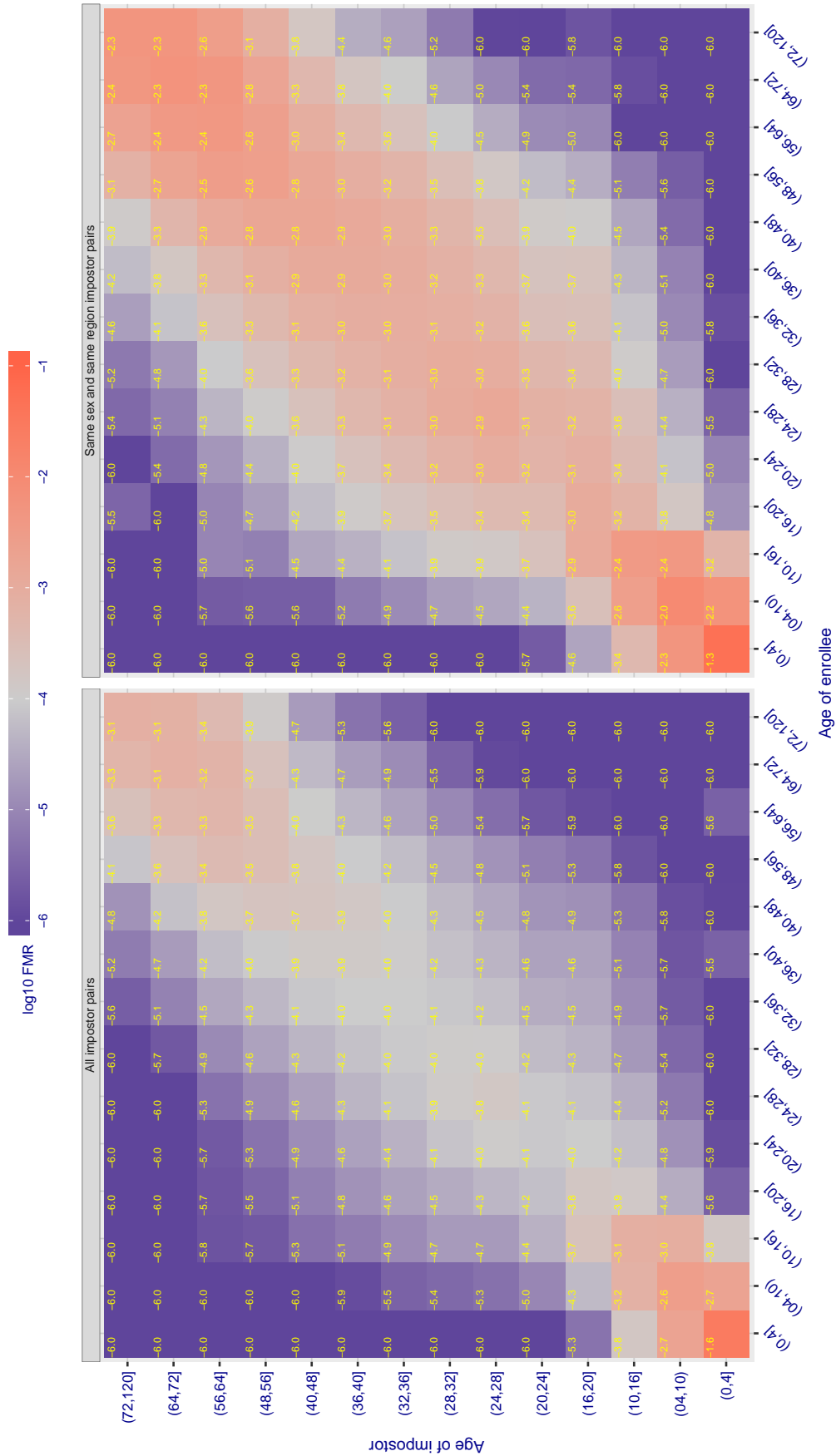


Figure 149: For algorithm neurotechnology-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = -0.660$ for algorithm noblis_000, giving $FMR(T) = 0.0001$ globally.

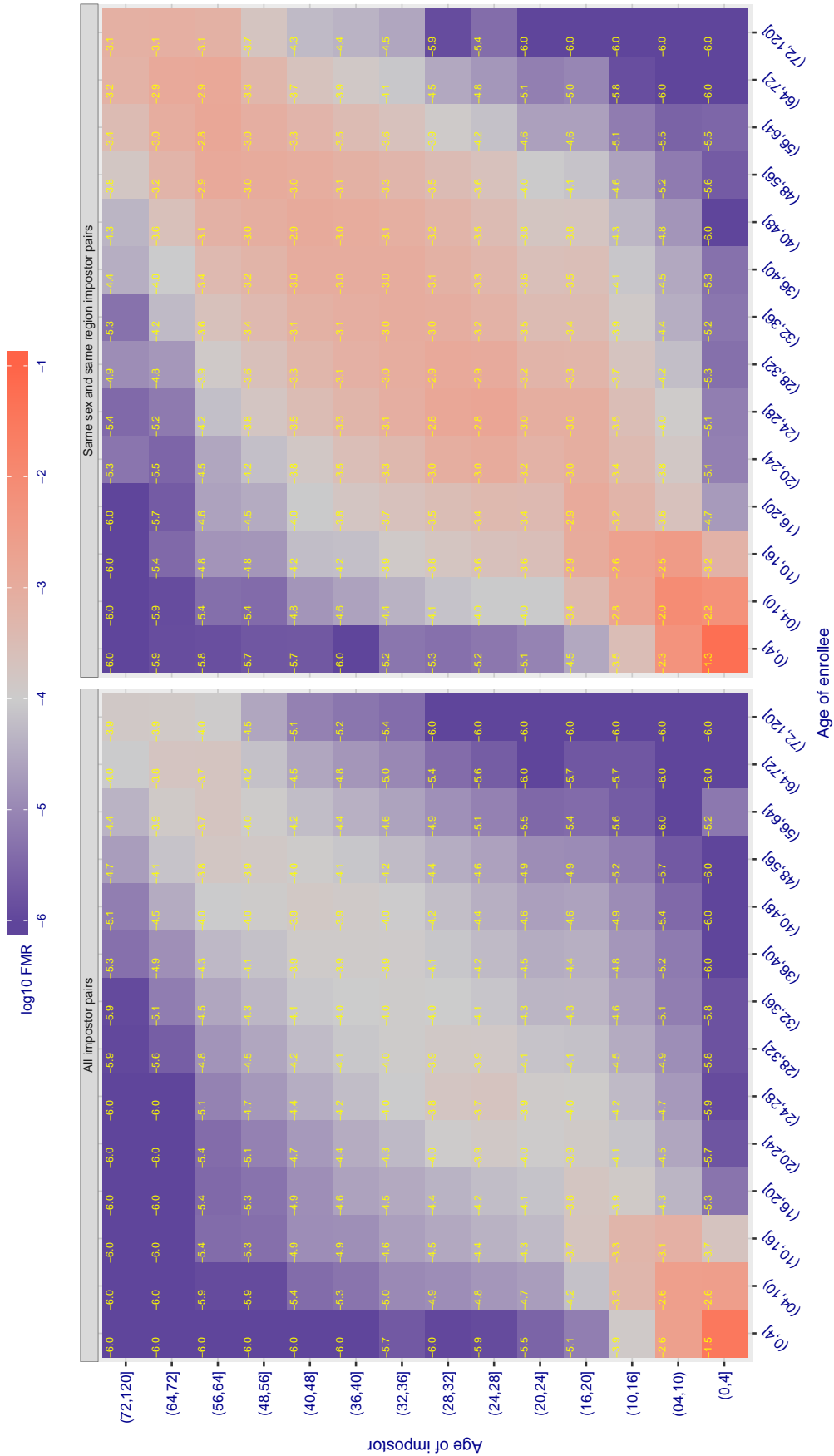


Figure 150: For algorithm noblis-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.099$ for algorithm ntechlab_002, giving $FMR(T) = 0.0001$ globally.

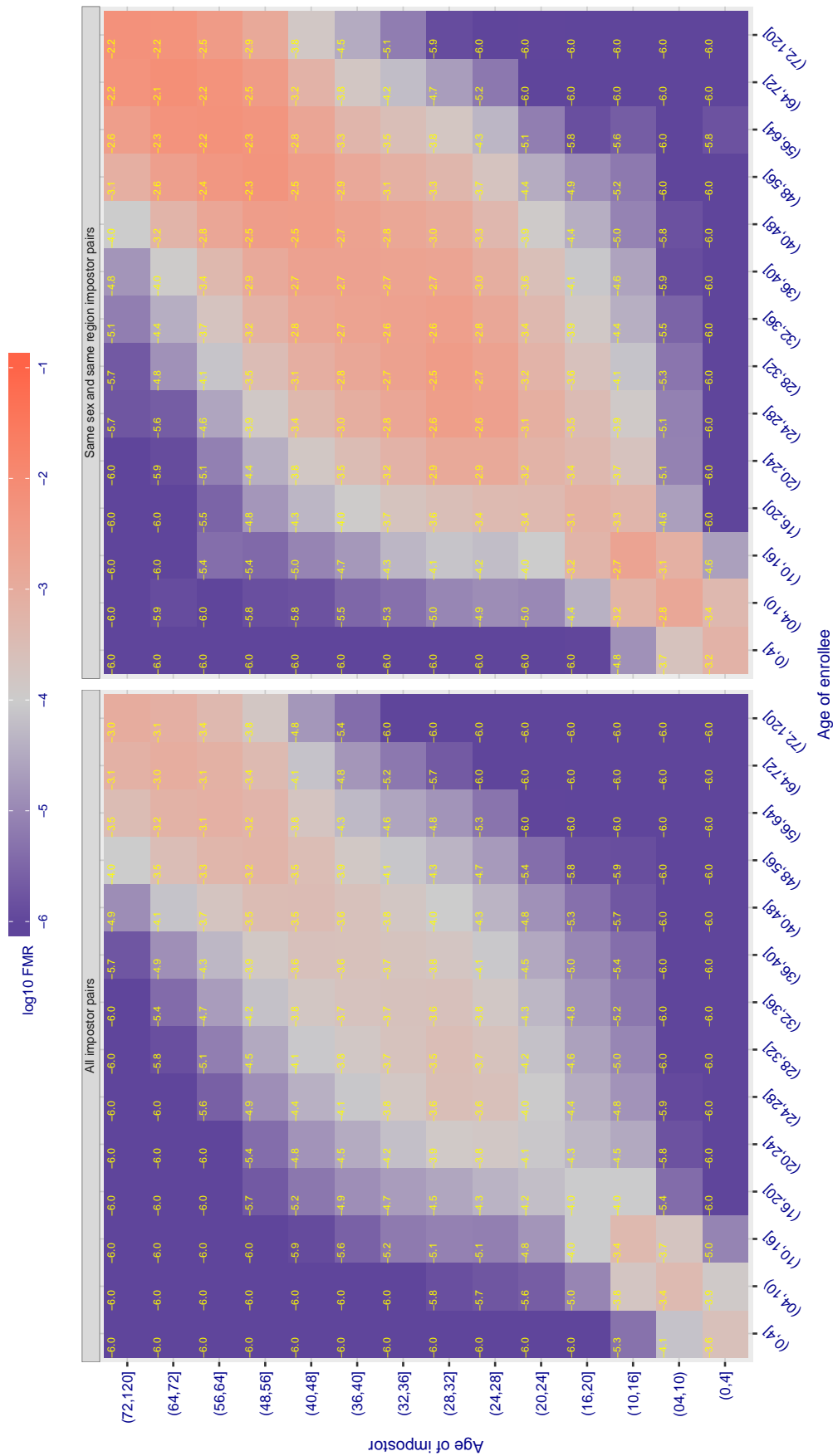


Figure 151: For algorithm ntechlab-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 3.759$ for algorithm ntechlab_003, giving $FMR(T) = 0.0001$ globally.

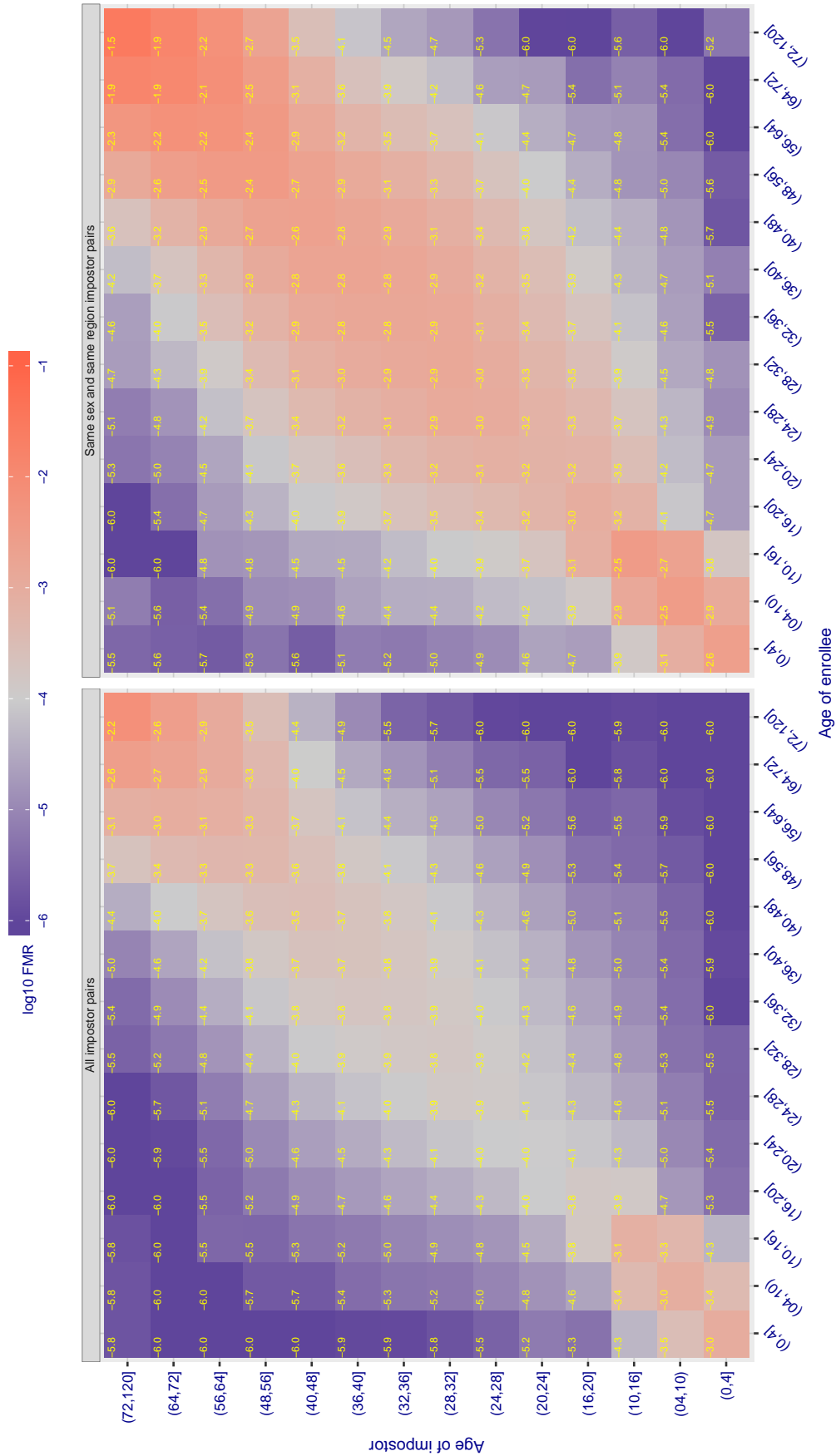


Figure 152: For algorithm ntechlab-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.839$ for algorithm pa_002, giving $FMR(T) = 0.0001$ globally.

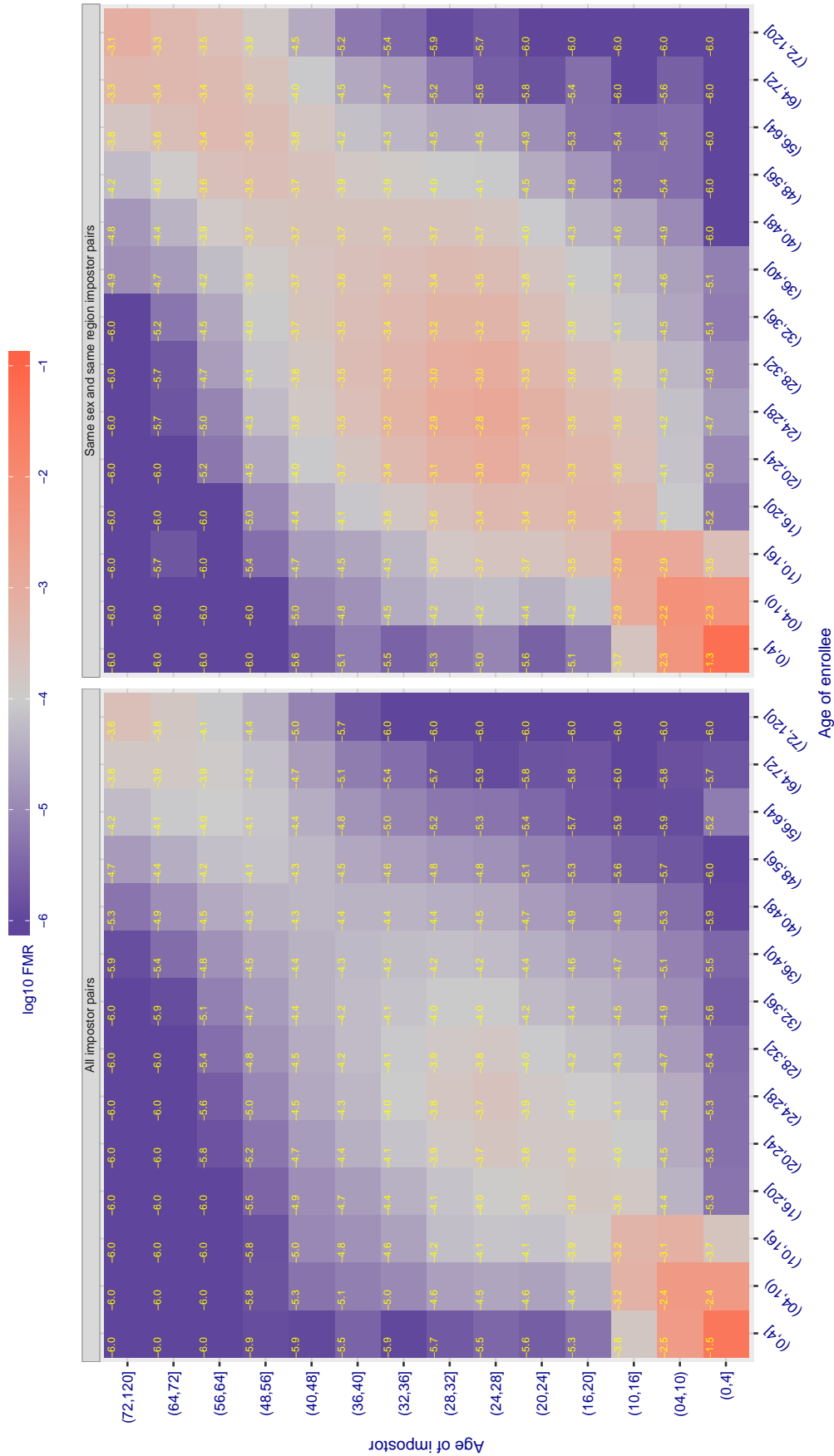


Figure 153: For algorithm pa-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.556$ for algorithm rankone_002, giving $FMR(T) = 0.0001$ globally.

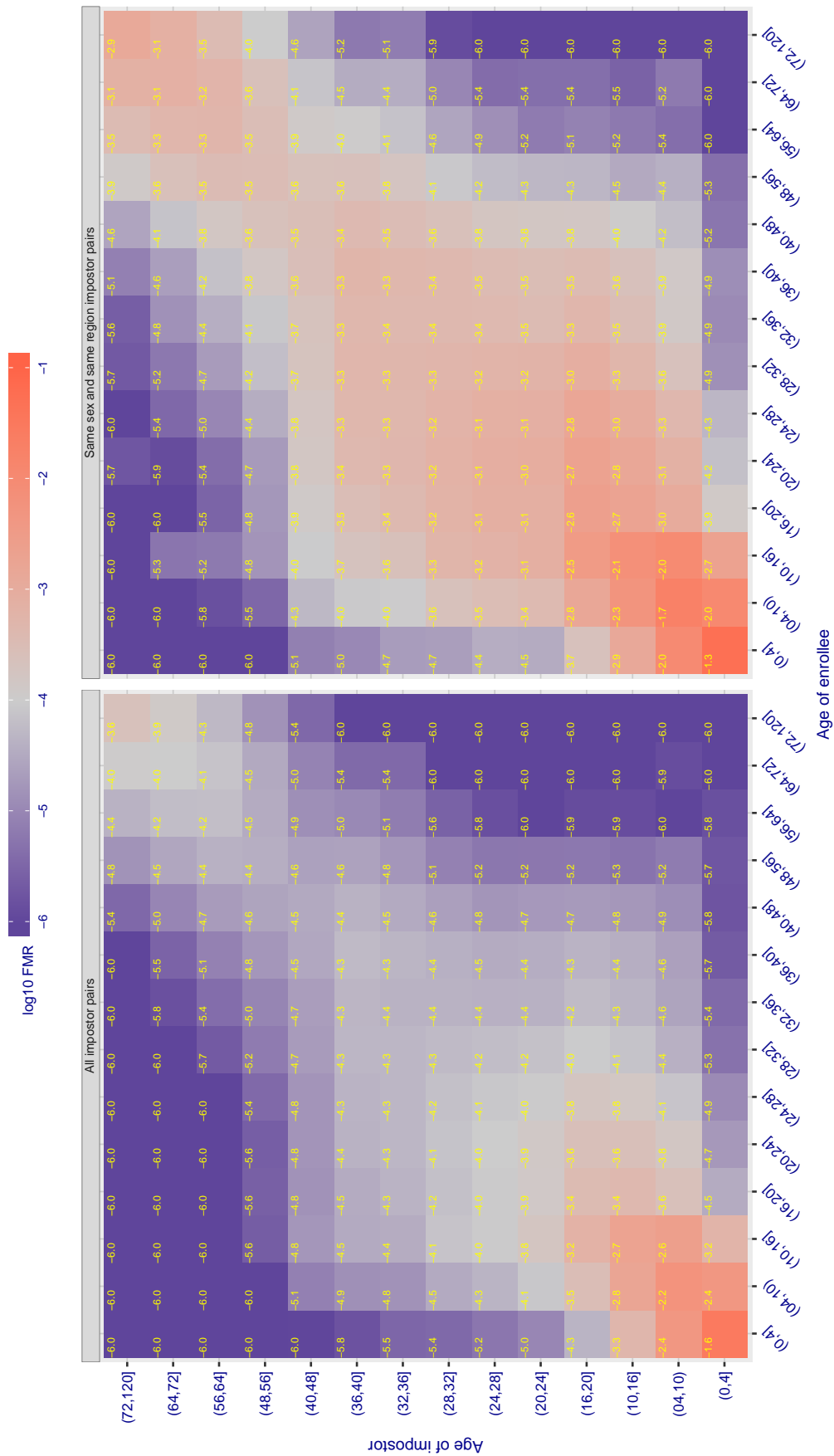


Figure 154: For algorithm rankone-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

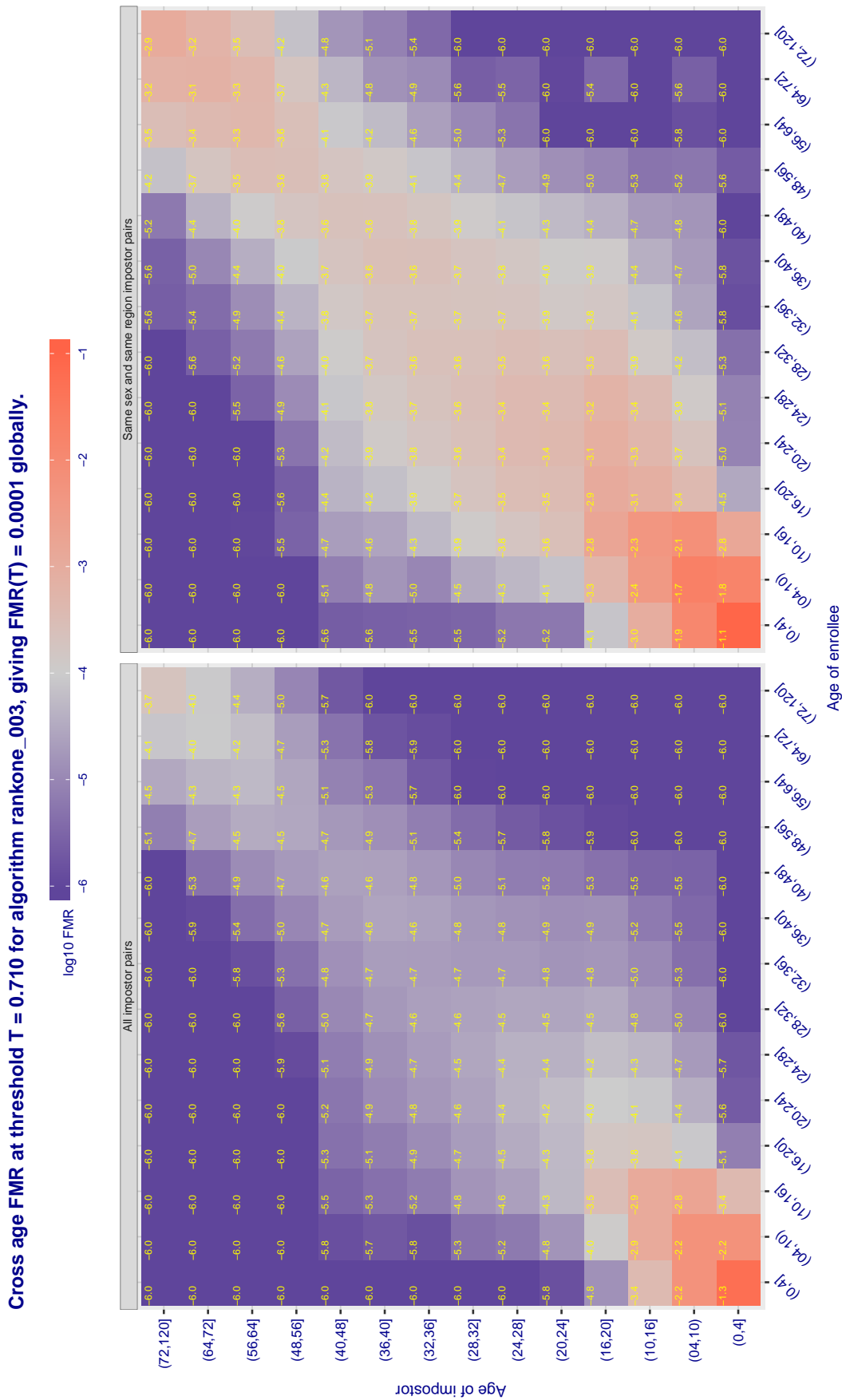


Figure 155: For algorithm rankone-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 80.766$ for algorithm samtech_000, giving $FMR(T) = 0.0001$ globally.

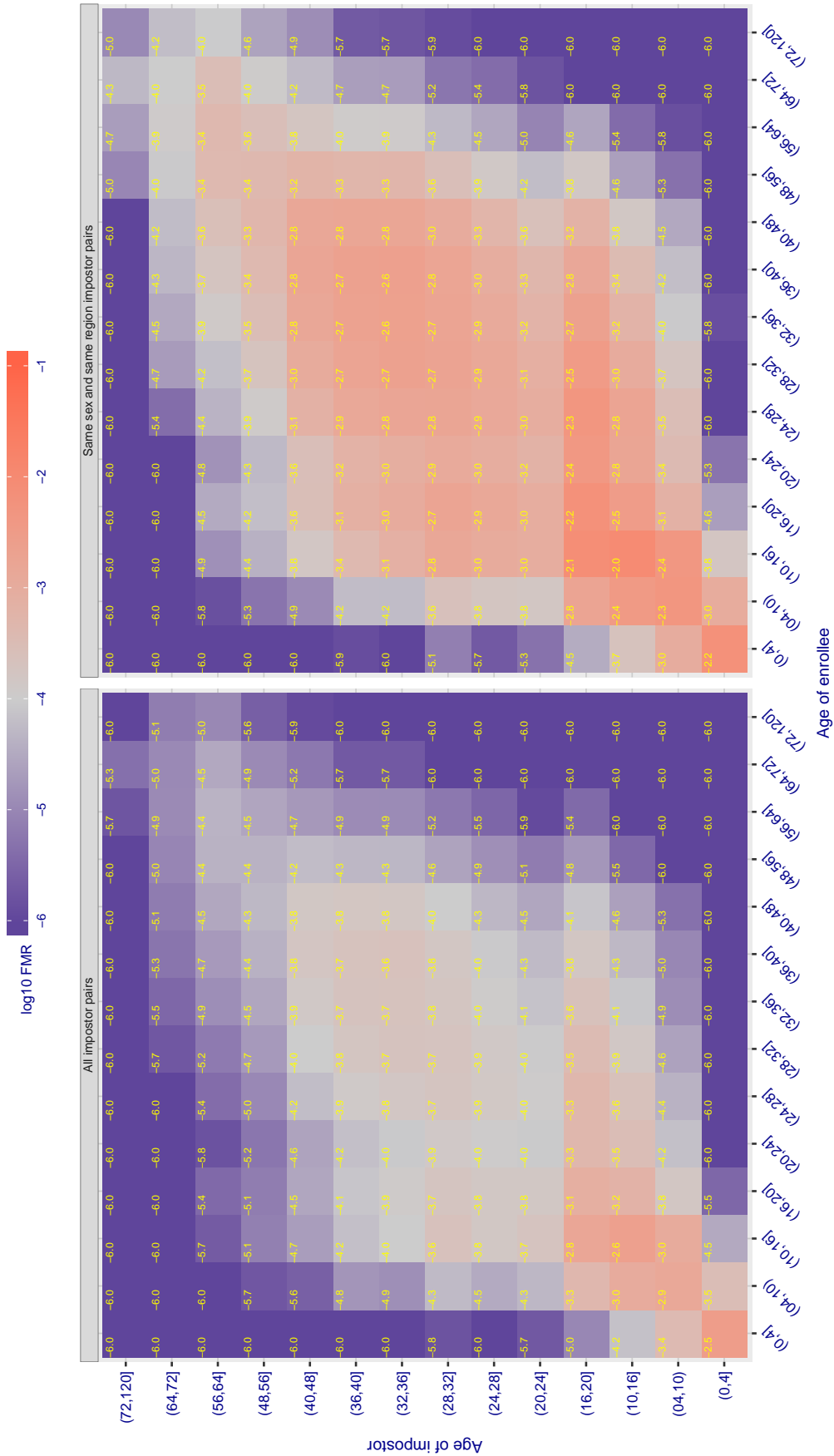


Figure 156: For algorithm samtech-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.970$ for algorithm shaman_000, giving $FMR(T) = 0.0001$ globally.

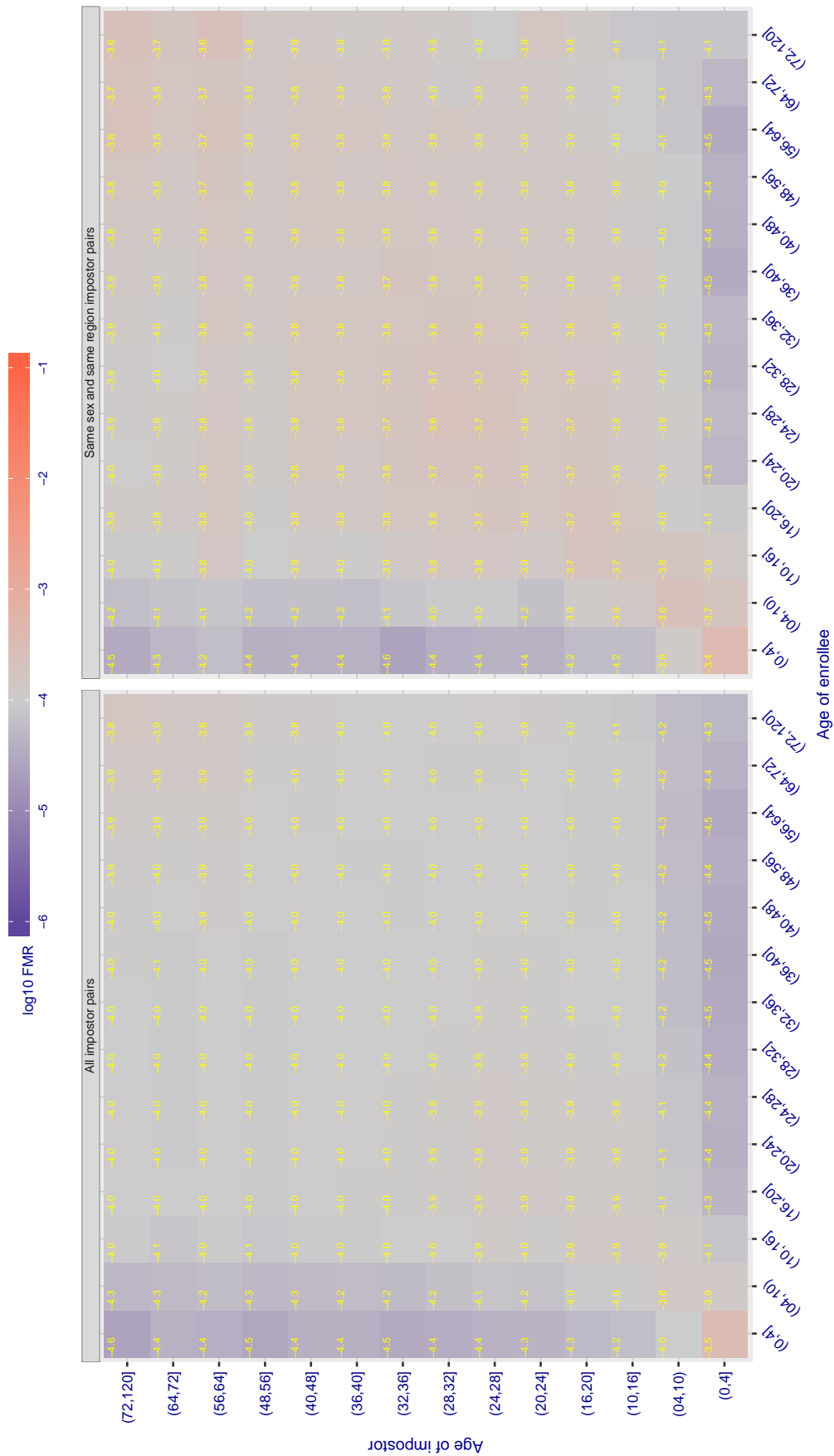


Figure 157: For algorithm shaman-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.725$ for algorithm shaman_001, giving $FMR(T) = 0.0001$ globally.

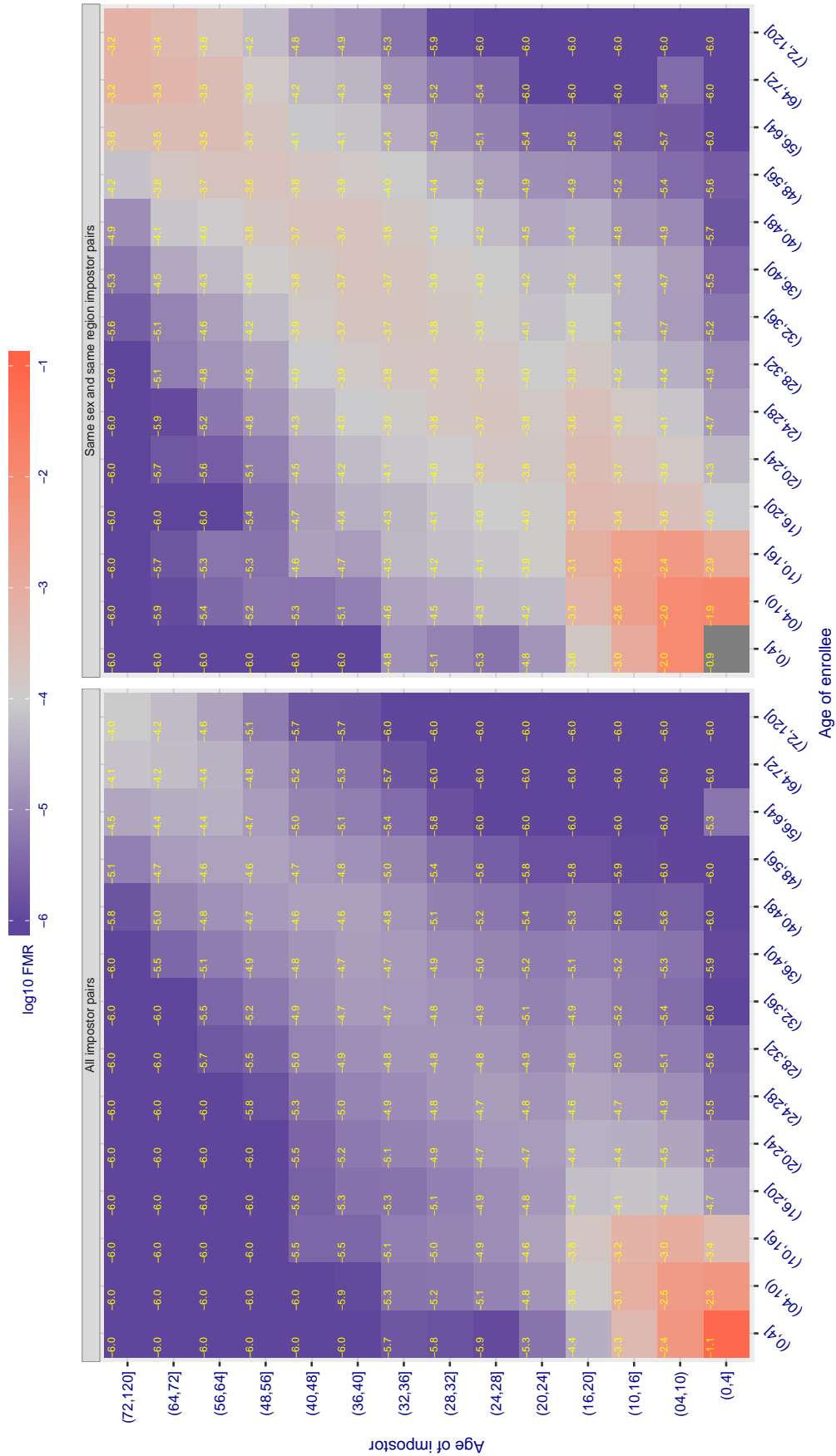


Figure 158: For algorithm shaman-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.929$ for algorithm `tevia_000`, giving $FMR(T) = 0.0001$ globally.

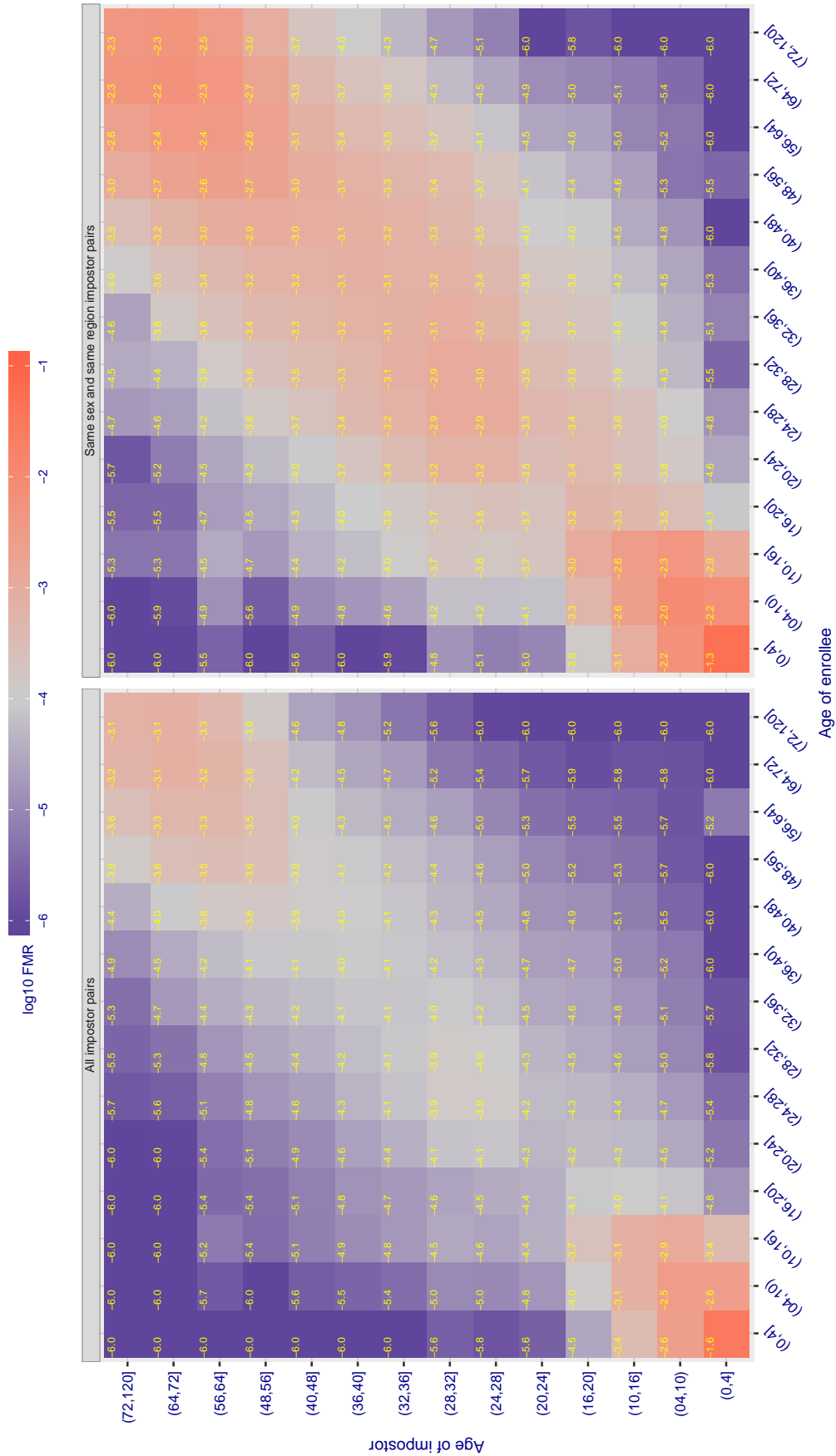


Figure 159: For algorithm `tevia_000` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.0001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 10.120$ for algorithm tongyitrans_001, giving $FMR(T) = 0.0001$ globally.

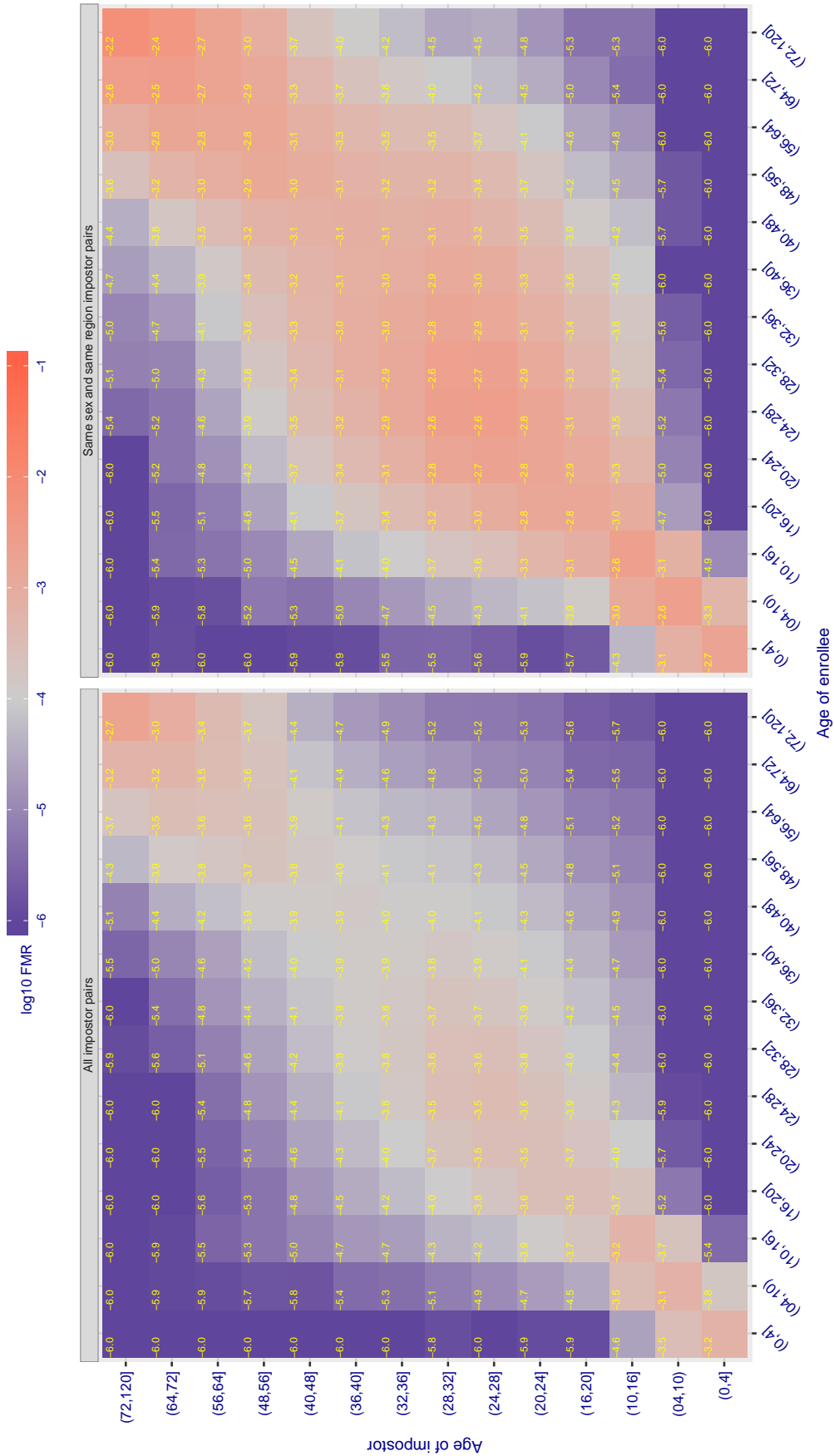


Figure 160: For algorithm `tongyitrans-001` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 3.971$ for algorithm tongyitrans_002, giving $FMR(T) = 0.0001$ globally.

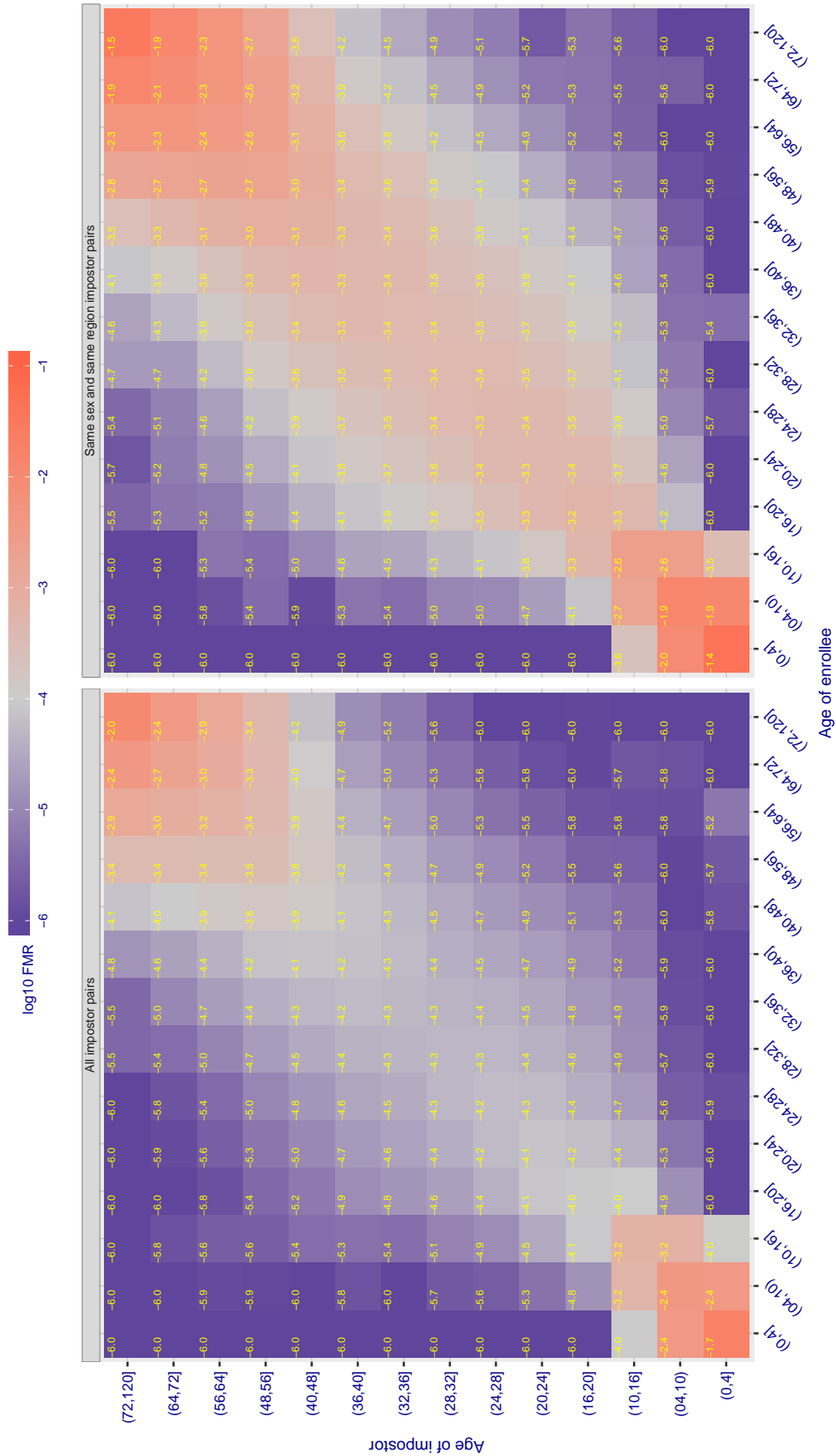


Figure 161: For algorithm `tongyitrans-002` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.644$ for algorithm toshiba_000, giving $FMR(T) = 0.0001$ globally.

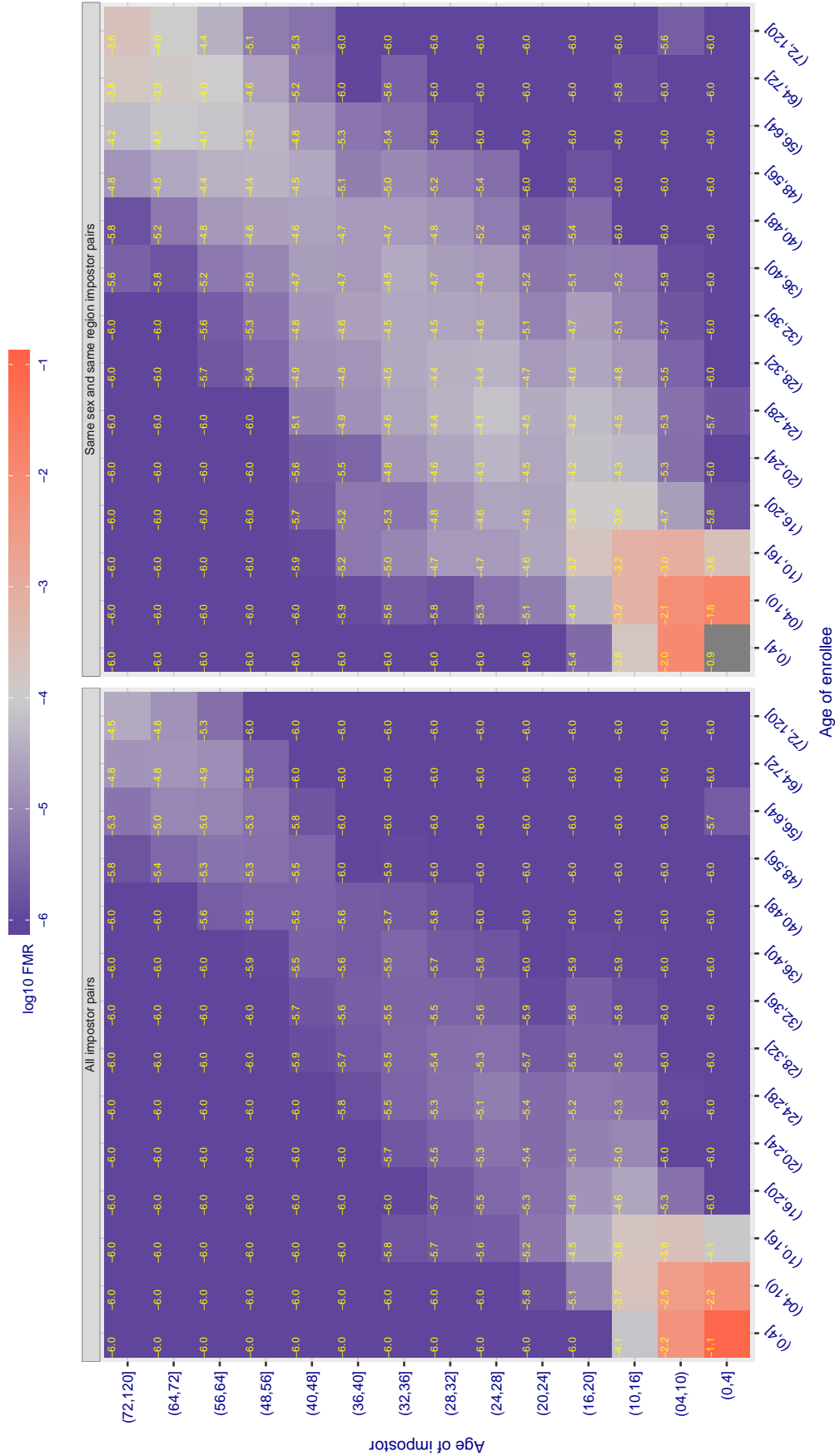


Figure 162: For algorithm toshiba-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.605$ for algorithm toshiba_001, giving $FMR(T) = 0.0001$ globally.

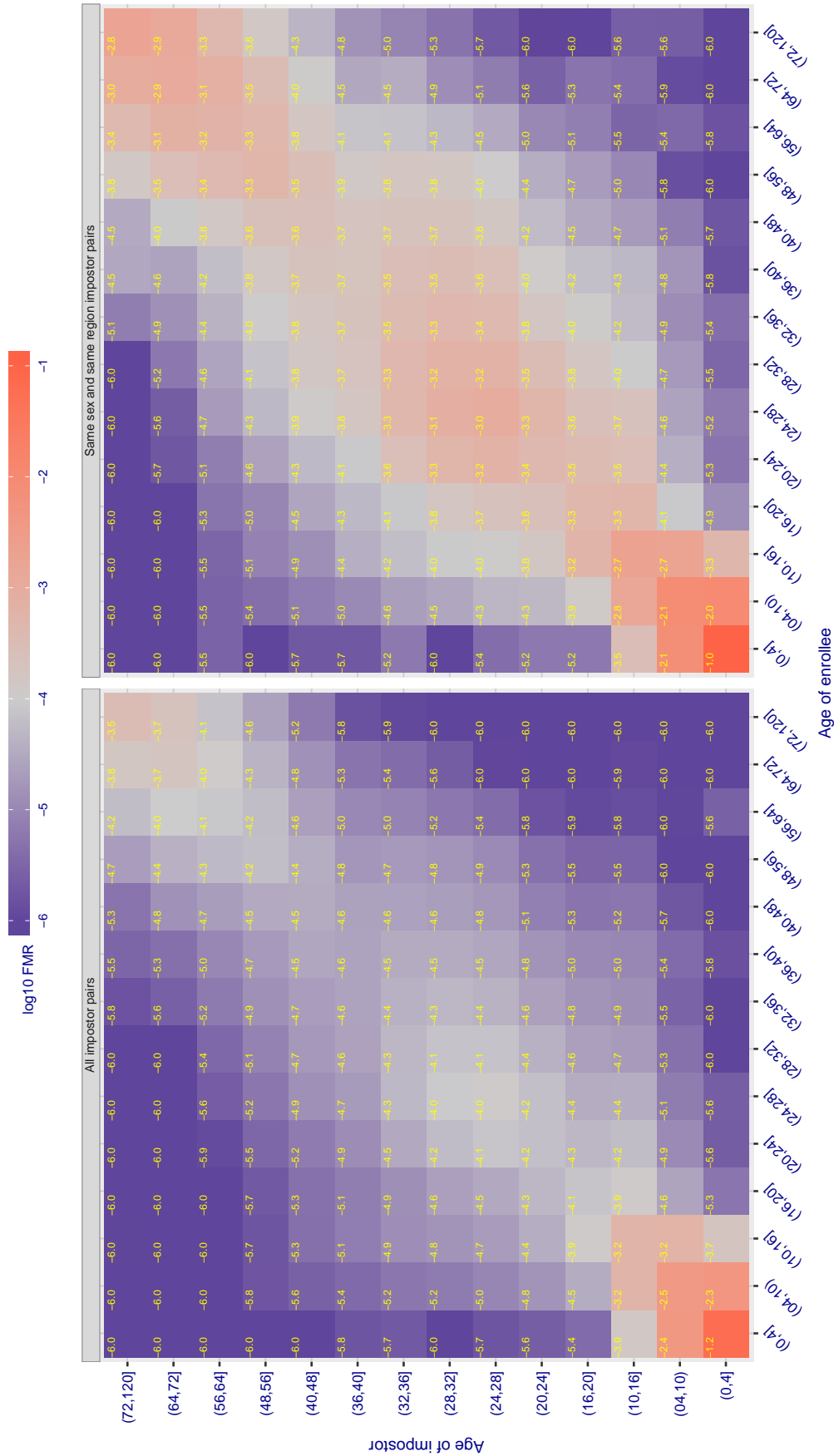


Figure 163: For algorithm toshiba-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

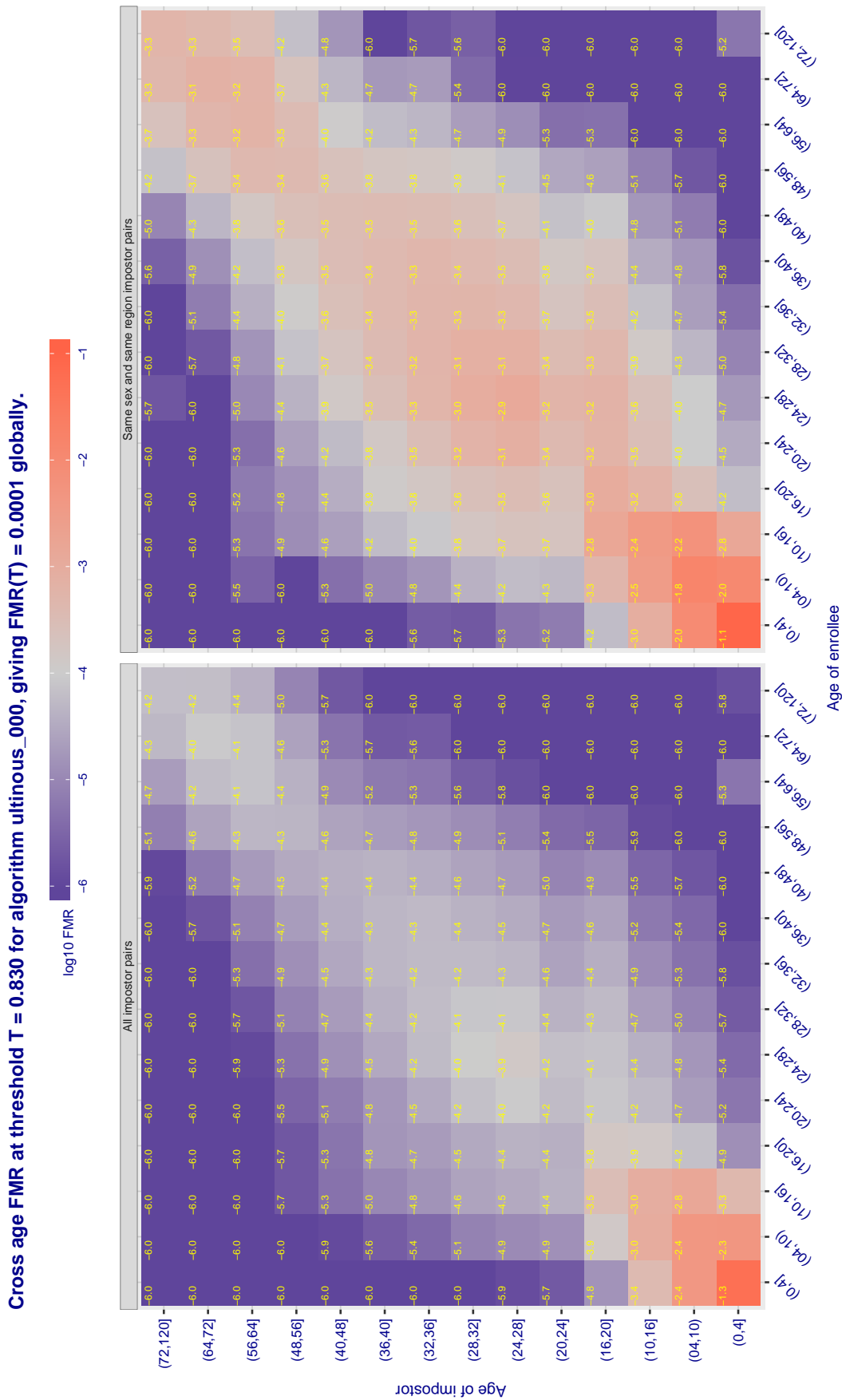


Figure 164: For algorithm ultinous-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.428$ for algorithm vcog_002, giving $FMR(T) = 0.0001$ globally.

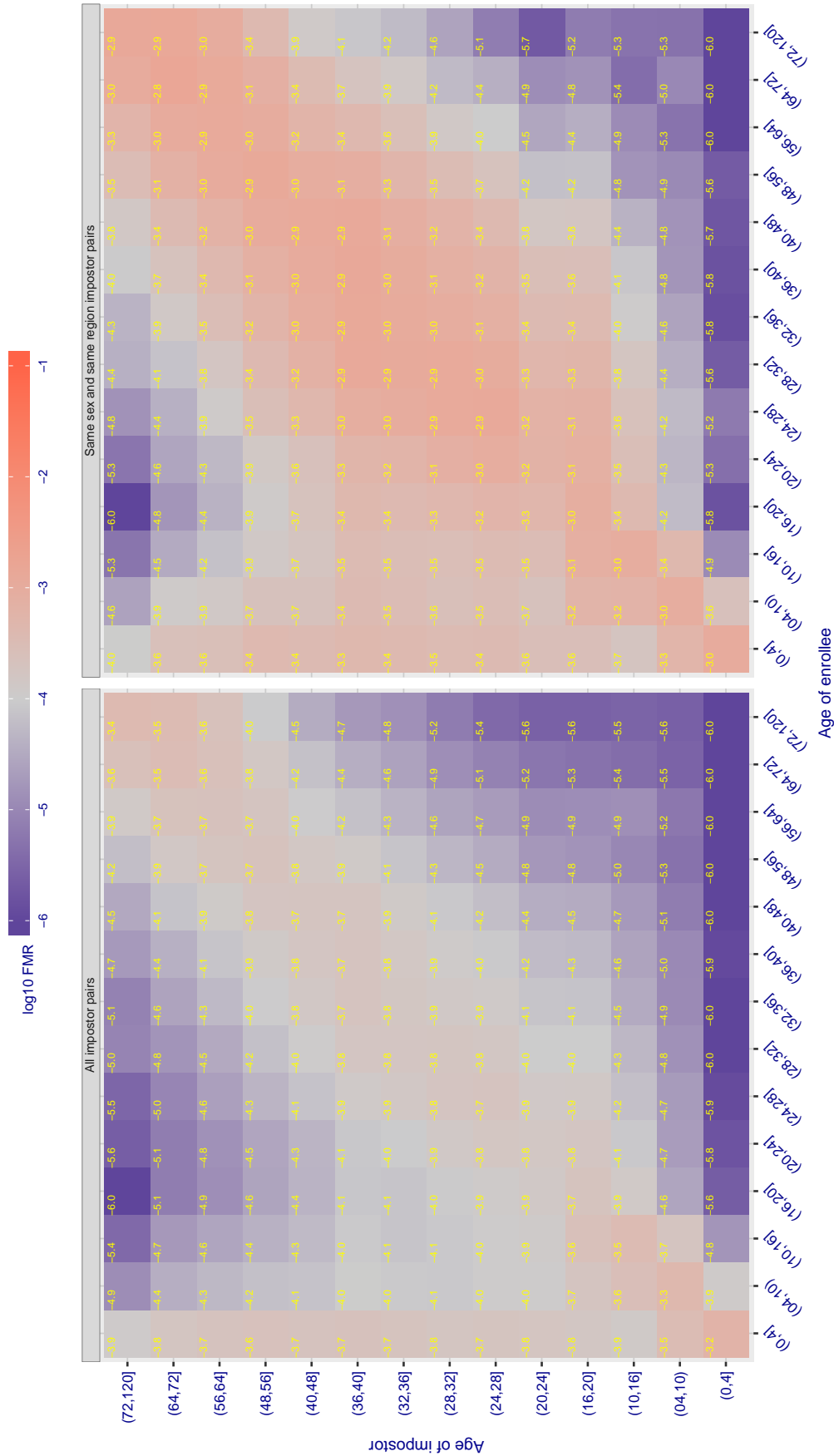


Figure 165: For algorithm vcog-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 4.315$ for algorithm `vigilantsolutions_002`, giving $FMR(T) = 0.0001$ globally.

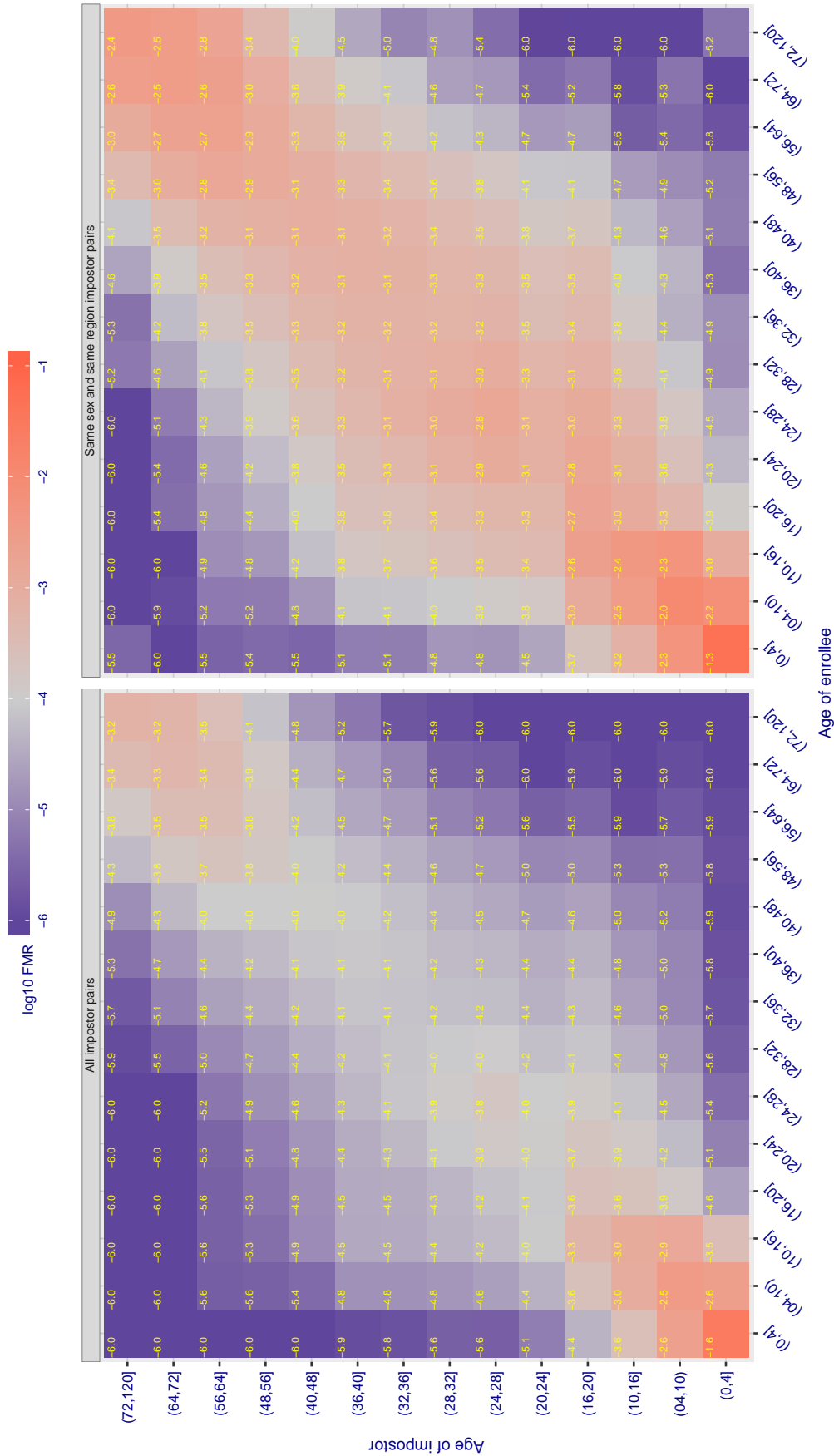


Figure 166: For algorithm `vigilantsolutions-002` operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 3.308$ for algorithm vigilantsolutions_003, giving $FMR(T) = 0.0001$ globally.

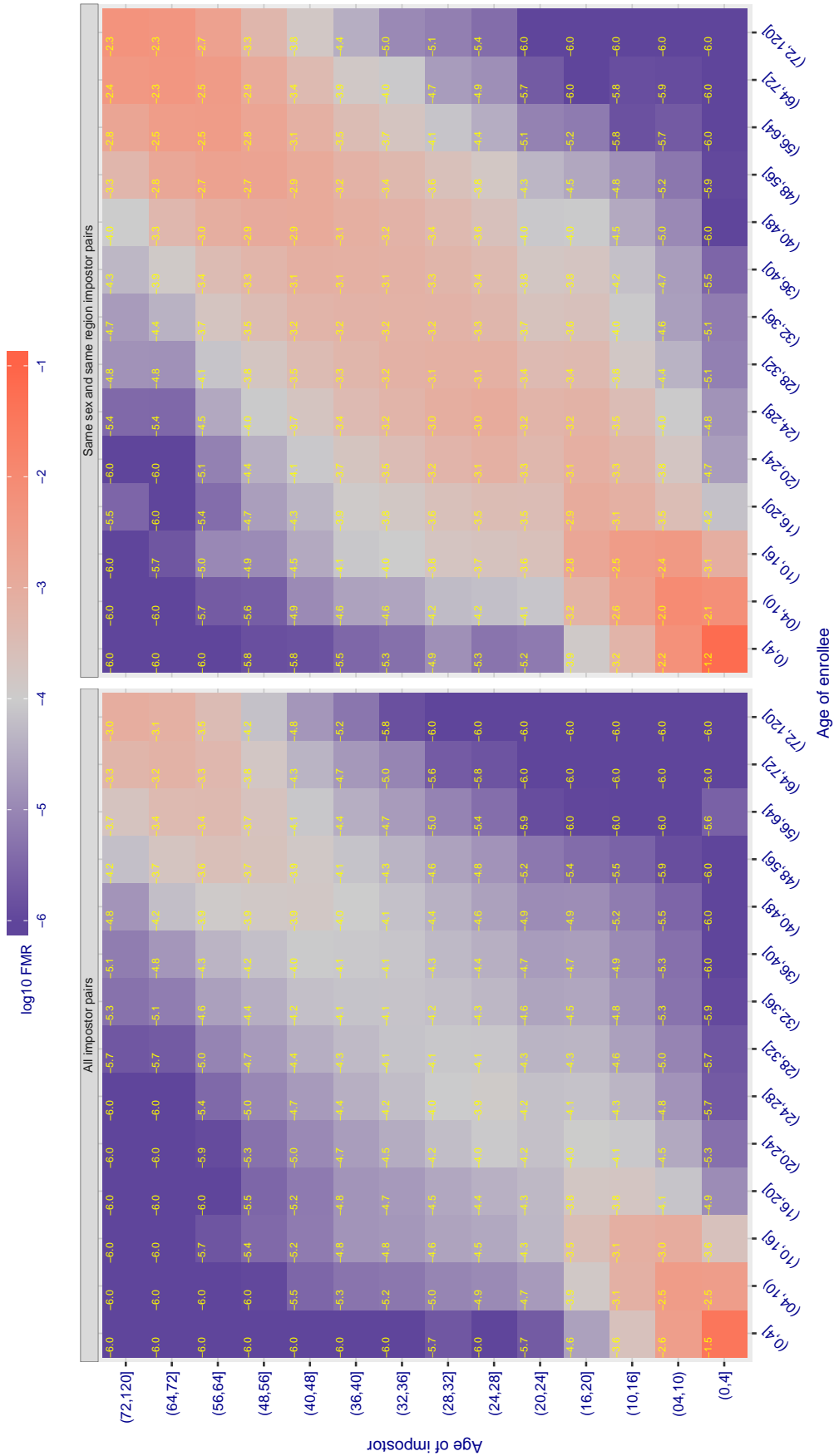


Figure 167: For algorithm vigilantsolutions-003 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.080$ for algorithm visionlabs_001, giving $FMR(T) = 0.0001$ globally.

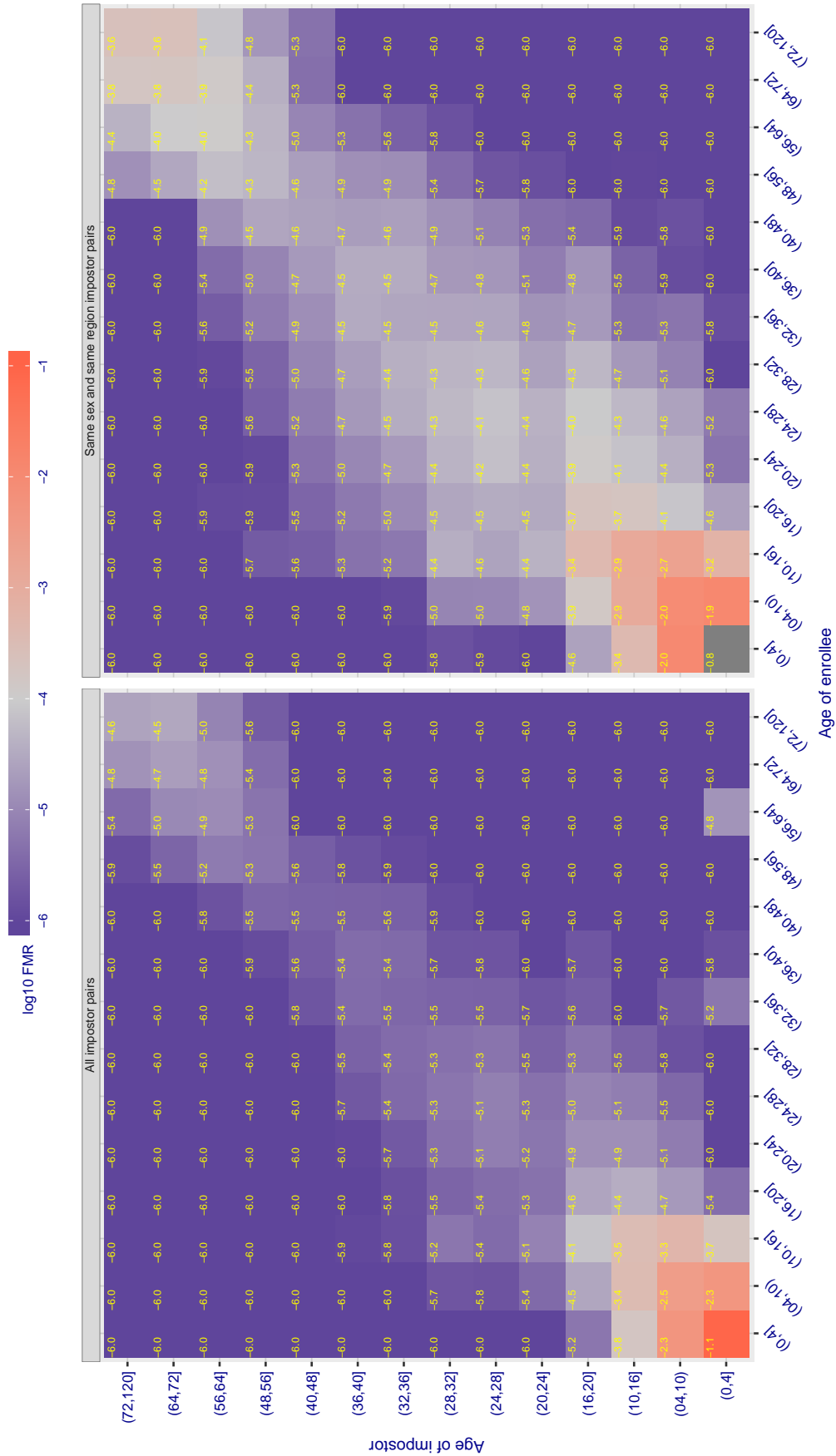


Figure 168: For algorithm visionlabs-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.794$ for algorithm visionlabs_002, giving $FMR(T) = 0.0001$ globally.

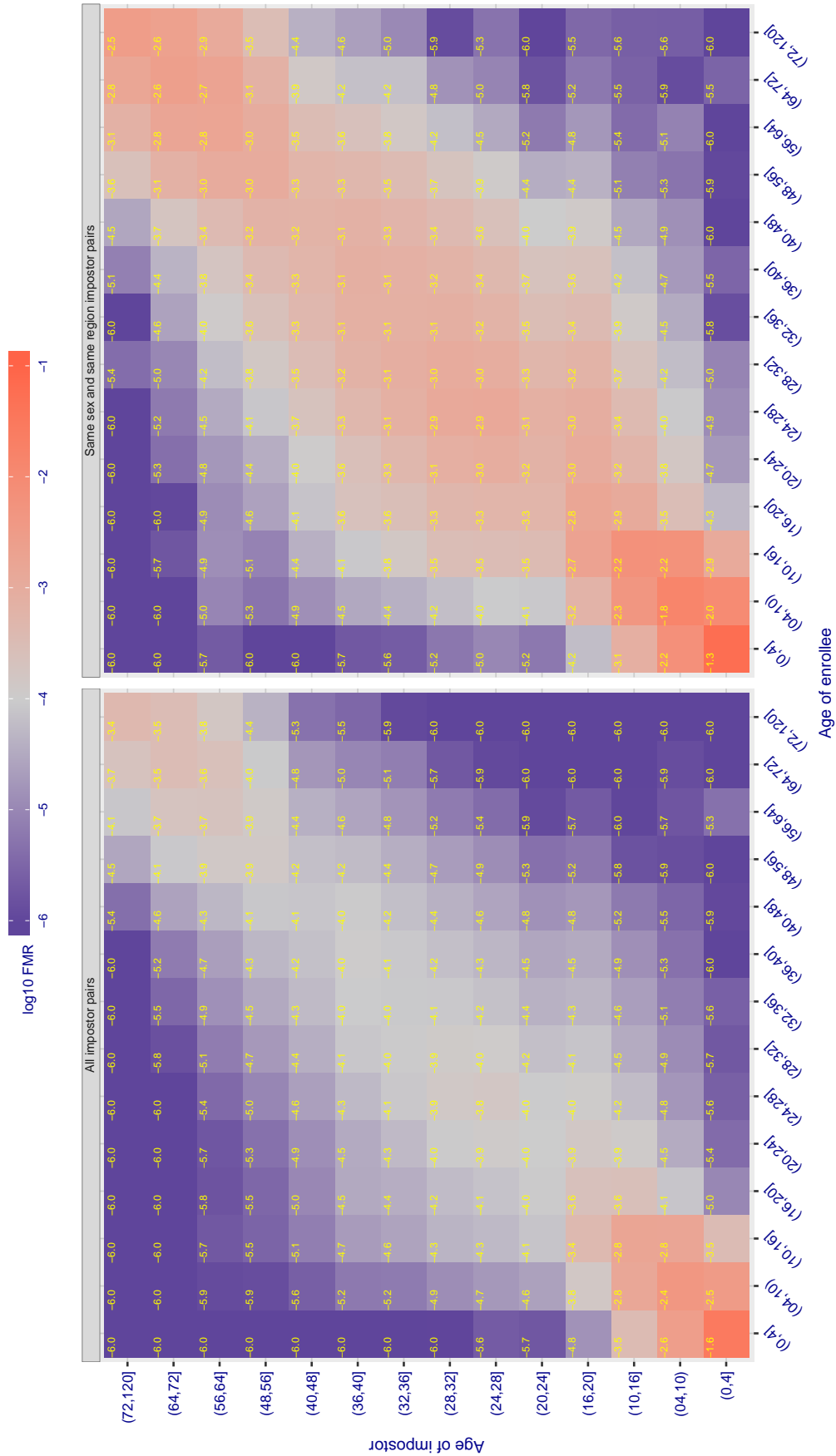


Figure 169: For algorithm visionlabs-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 0.867$ for algorithm vocord_002, giving $FMR(T) = 0.0001$ globally.

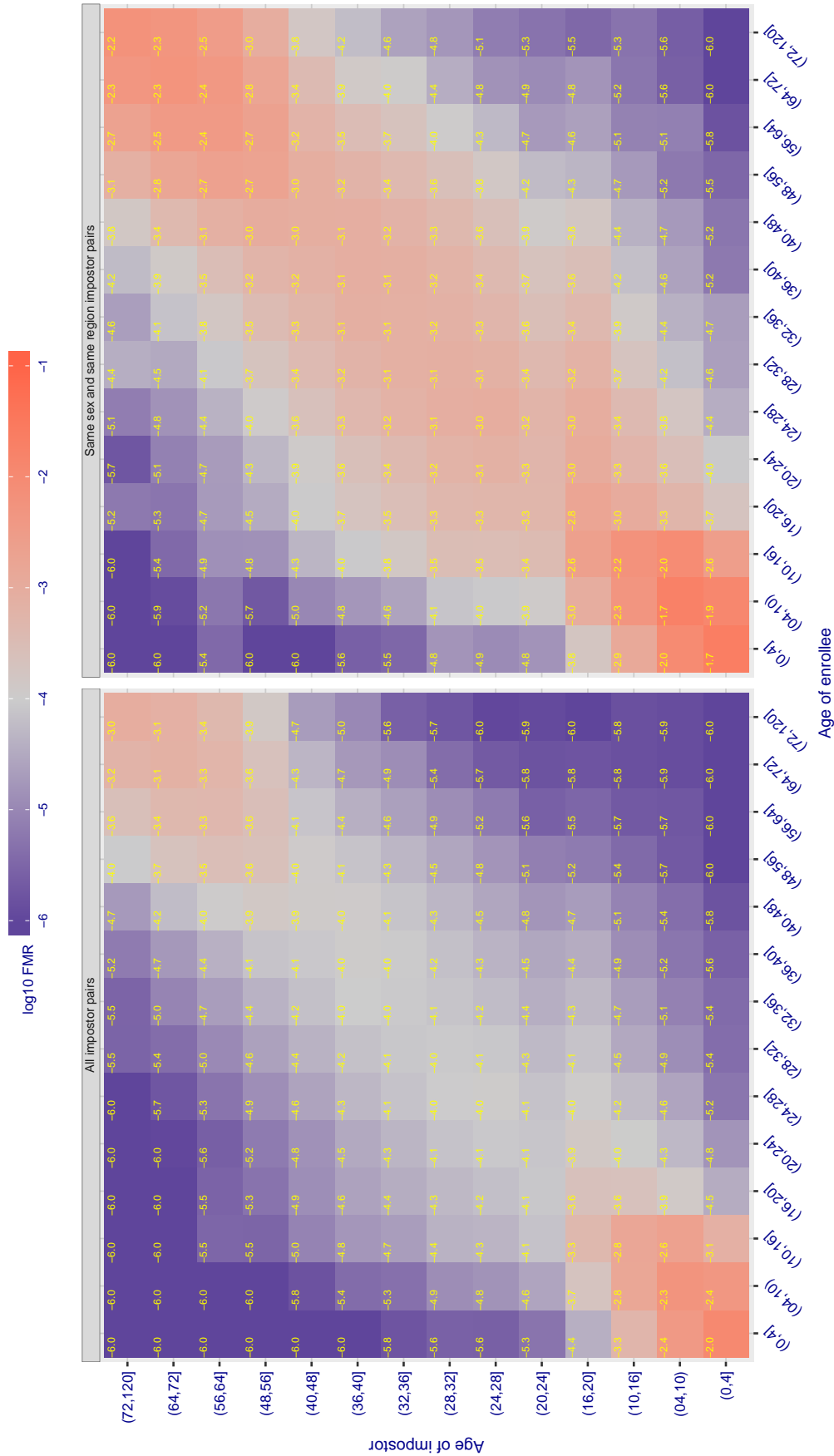


Figure 170: For algorithm vocord-002 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 6.196$ for algorithm yisheng_000, giving $FMR(T) = 0.0001$ globally.

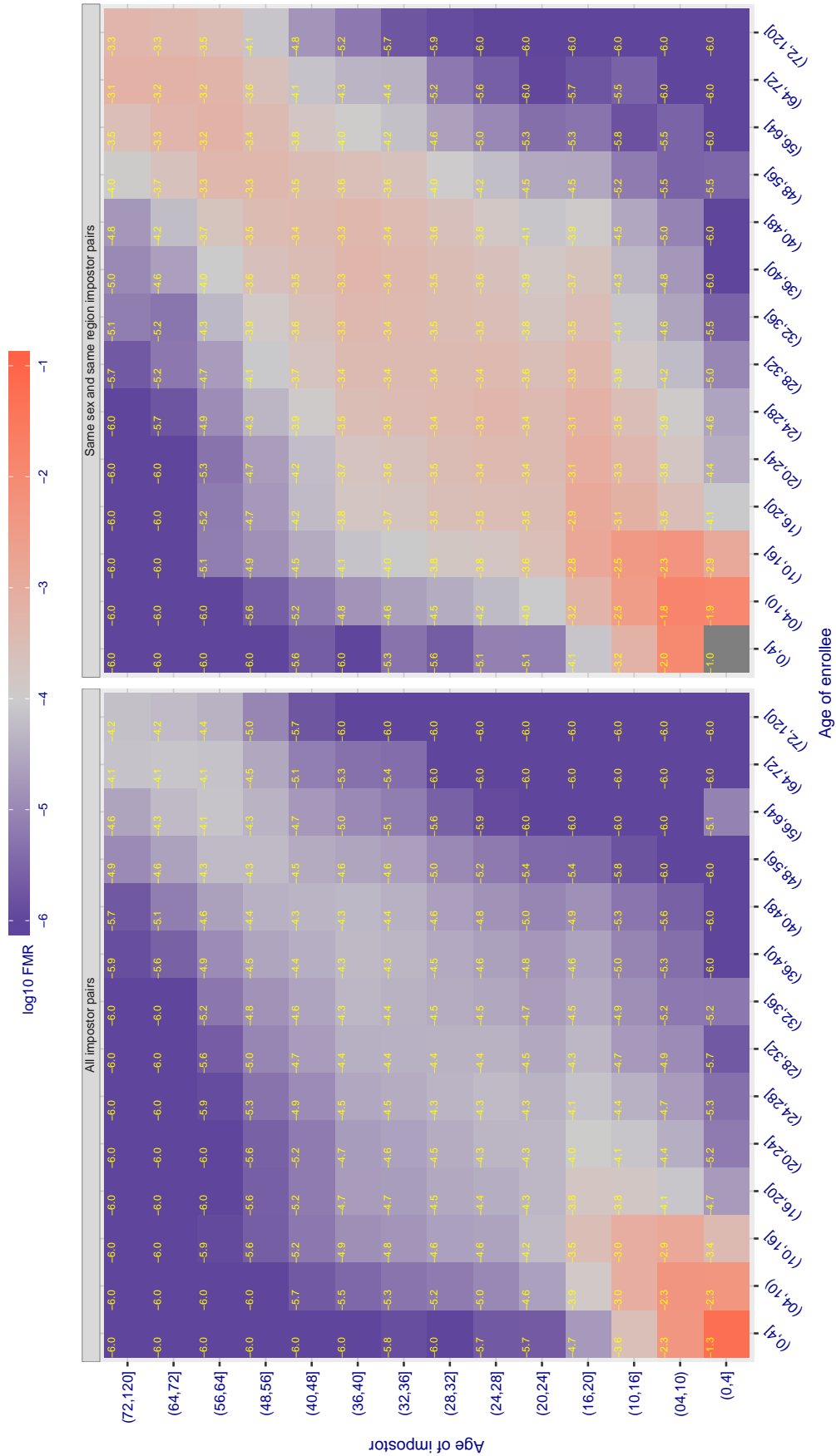


Figure 171: For algorithm yisheng-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 6.278$ for algorithm yisheng_001, giving $FMR(T) = 0.0001$ globally.

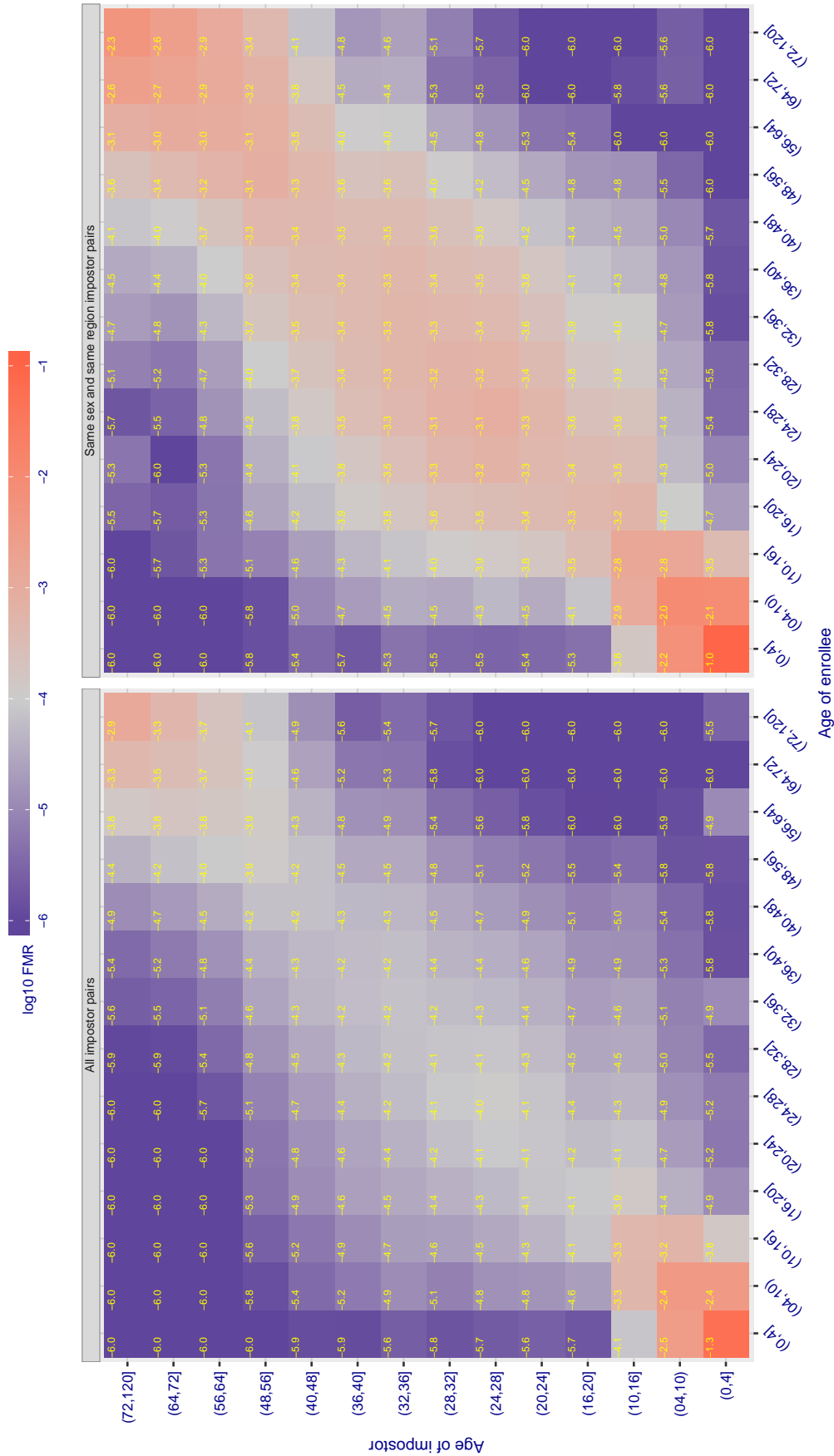


Figure 172: For algorithm yisheng-001 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Cross age FMR at threshold $T = 10.098$ for algorithm yitu_000, giving $FMR(T) = 0.0001$ globally.

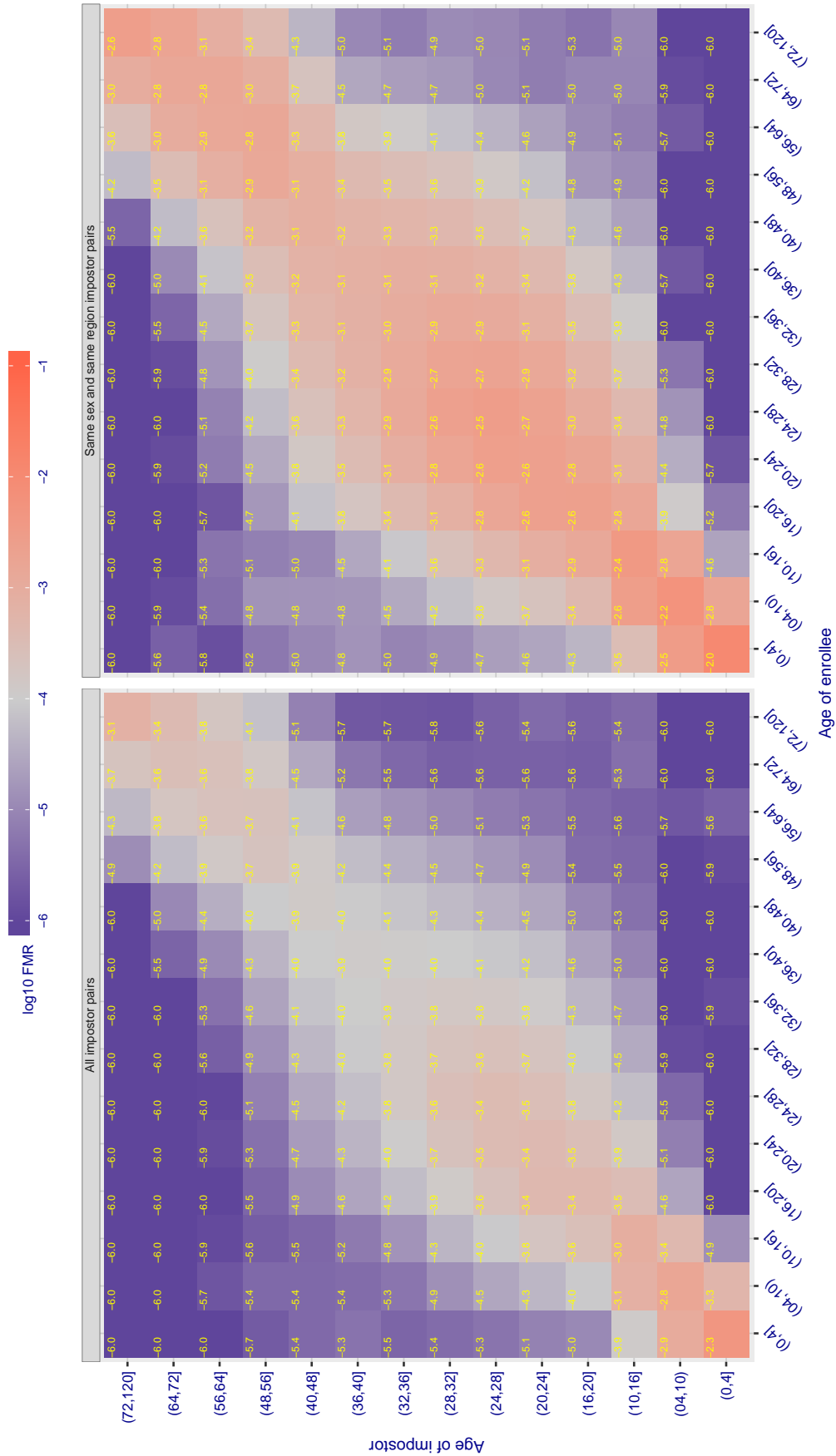


Figure 173: For algorithm yitu-000 operating on visa images, the heatmap shows false match observed over impostor comparisons of faces from different individuals who have the given age pair. False matches are counted against a recognition threshold fixed globally to give $FMR = 0.001$ over all $O(10^{10})$ impostor comparisons. The text in each box gives the same quantity as that coded by the color. Light colors present a security vulnerability to, for example, a passport gate.

Accuracy Terms + Definitions

In biometrics, Type II errors occur when two samples of one person do not match – this is called a **false negative**. Correspondingly, Type I errors occur when samples from two persons do match – this is called a **false positive**. Matches are declared by a biometric system when the native comparison score from the recognition algorithm meets some **threshold**. Comparison scores can be either **similarity scores**, in which case higher values indicate that the samples are more likely to come from the same person, or **dissimilarity scores**, in which case higher values indicate different people. Similarity scores are traditionally computed by **fingerprint** and **face** recognition algorithms, while dissimilarities are used in **iris recognition**. In some cases, the dissimilarity score is a distance; this applies only when **metric** properties are obeyed. In any case, scores can be either **mate** scores, coming from a comparison of one person's samples, or **nonmate** scores, coming from comparison of different persons' samples. The words **genuine** or **authentic** are synonyms for mate, and the word **impostor** is used a synonym for nonmate. The words mate and nonmate are traditionally used in identification applications (such as law enforcement search, or background checks) while genuine and impostor are used in verification applications (such as access control).

A **error tradeoff** characteristic represents the tradeoff between Type II and Type I classification errors. For verification this plots false non-match rate (FNMR) vs. false match rate (FMR) parametrically with T.

The error tradeoff plots are often called **detection error tradeoff (DET)** characteristics or **receiver operating characteristic (ROC)**. These serve the same function but differ, for example, in plotting the complement of an error rate (e.g. $TMR = 1 - FNMR$) and in transforming the axes most commonly using logarithms, to show multiple decades of FMR. More rarely, the function might be the inverse Gaussian function.

More detail and generality is provided in formal biometrics testing standards, see the various parts of [ISO/IEC 19795 Biometrics Testing and Reporting](#). More terms, including and beyond those to do with accuracy, see [ISO/IEC 2382-37 Information technology -- Vocabulary -- Part 37: Harmonized biometric vocabulary](#)

