

Fig. 1

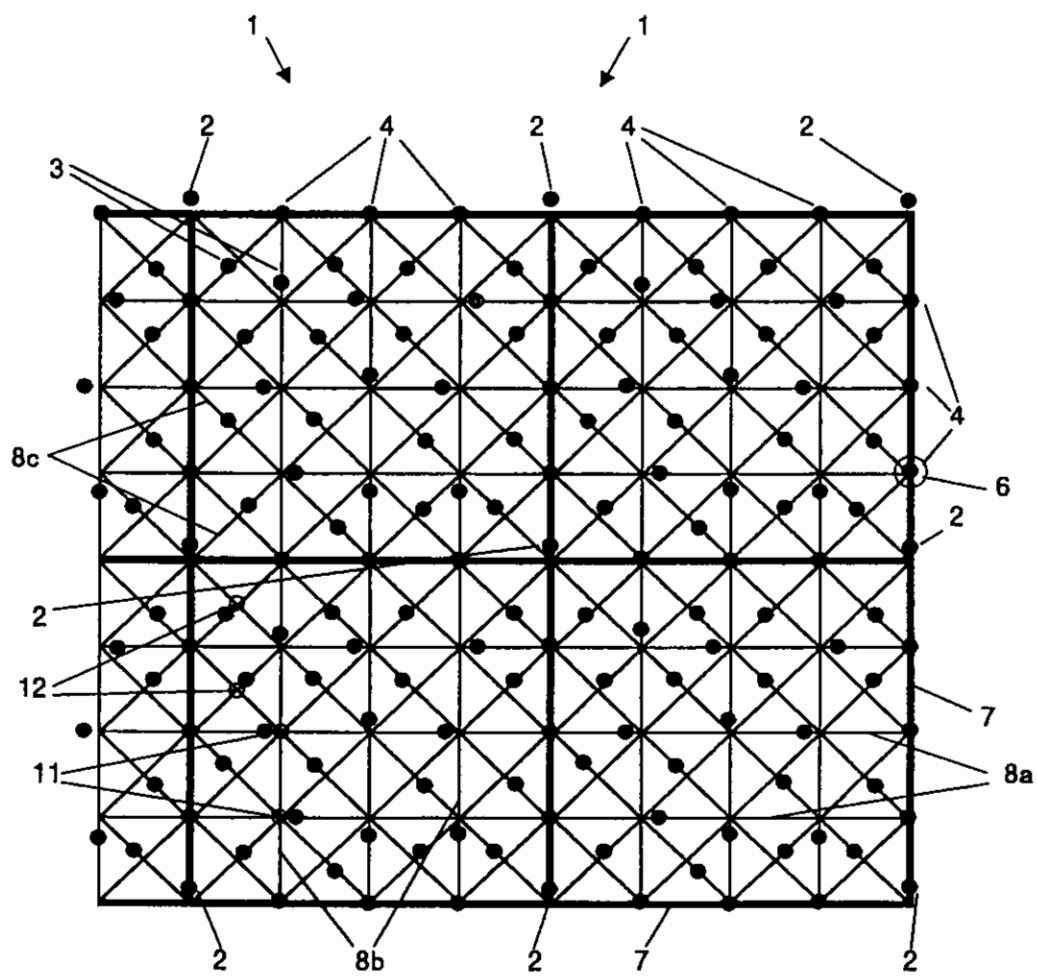


Fig. 2

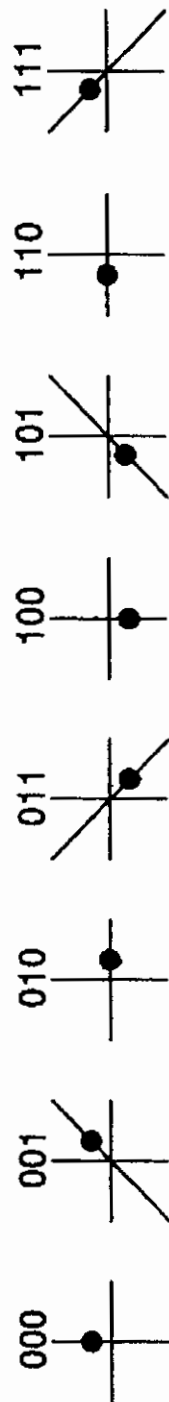


Fig. 3

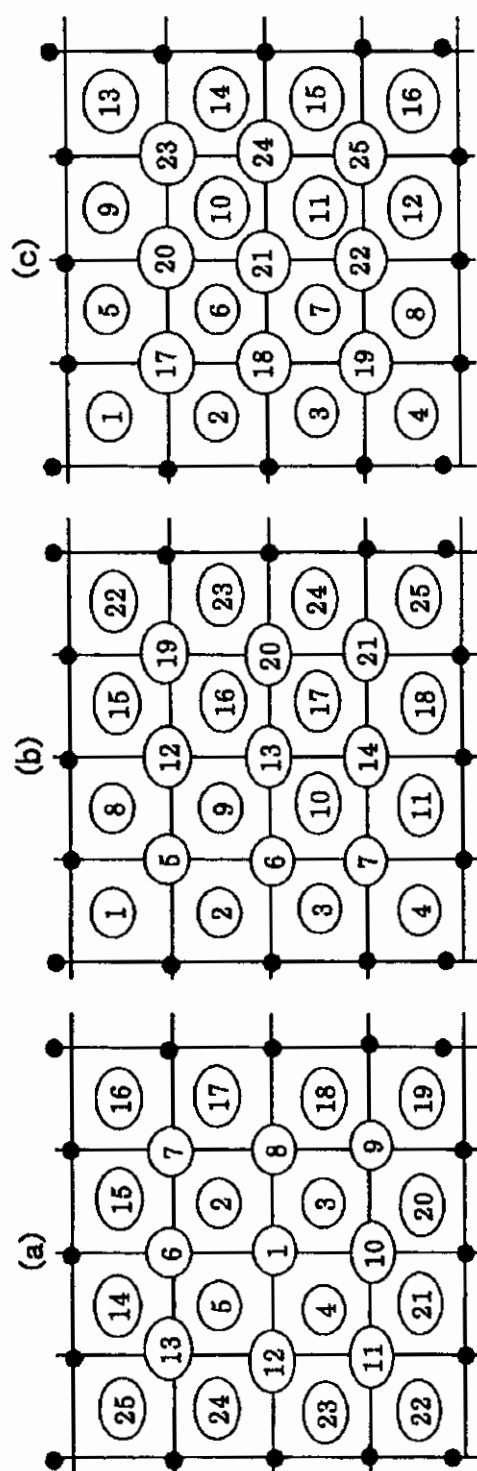


Fig. 4

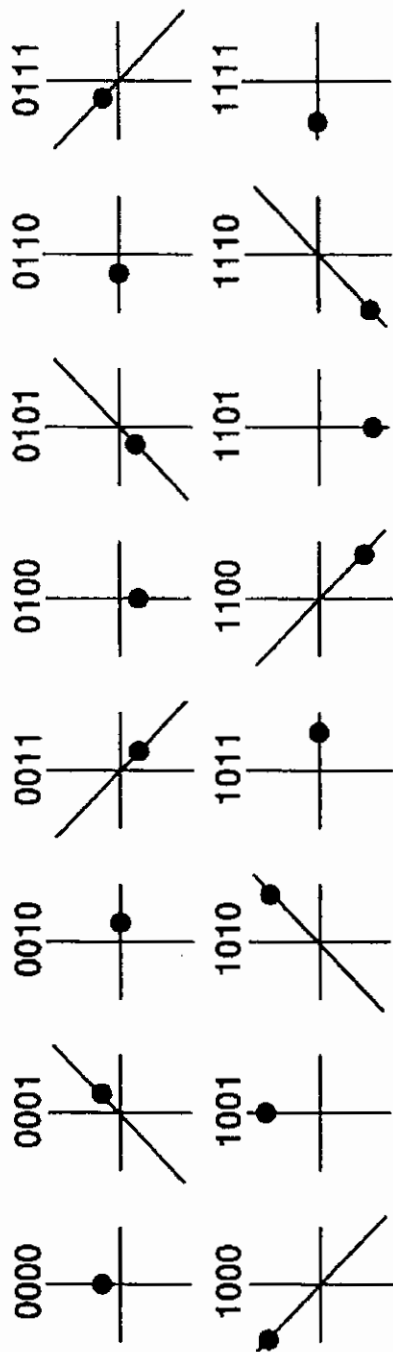


Fig. 5

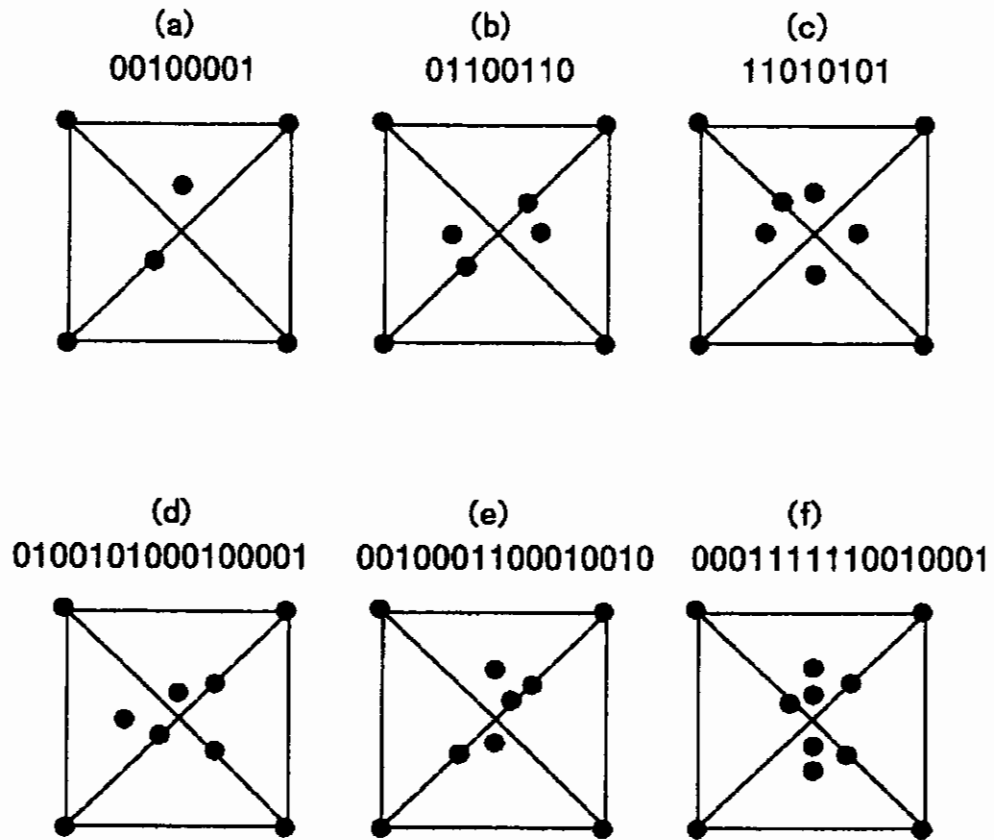


Fig. 6

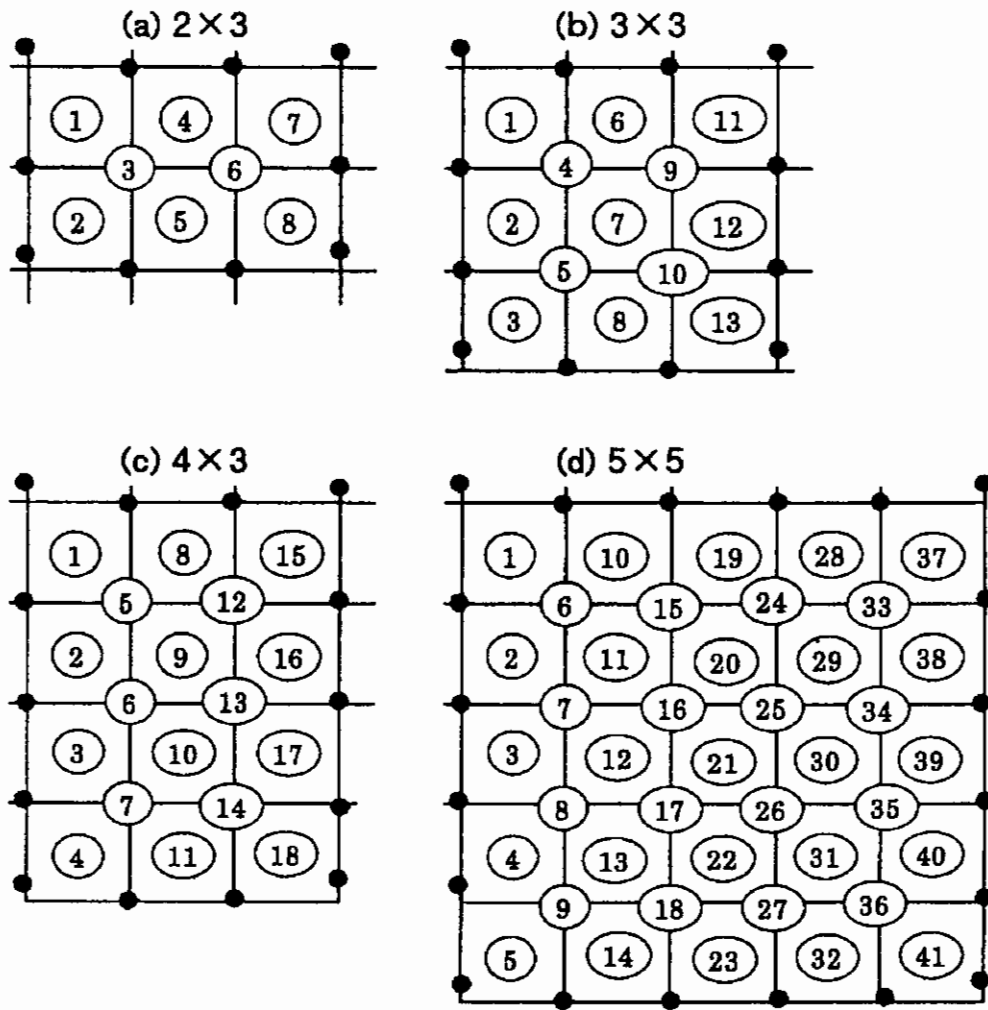


Fig. 7

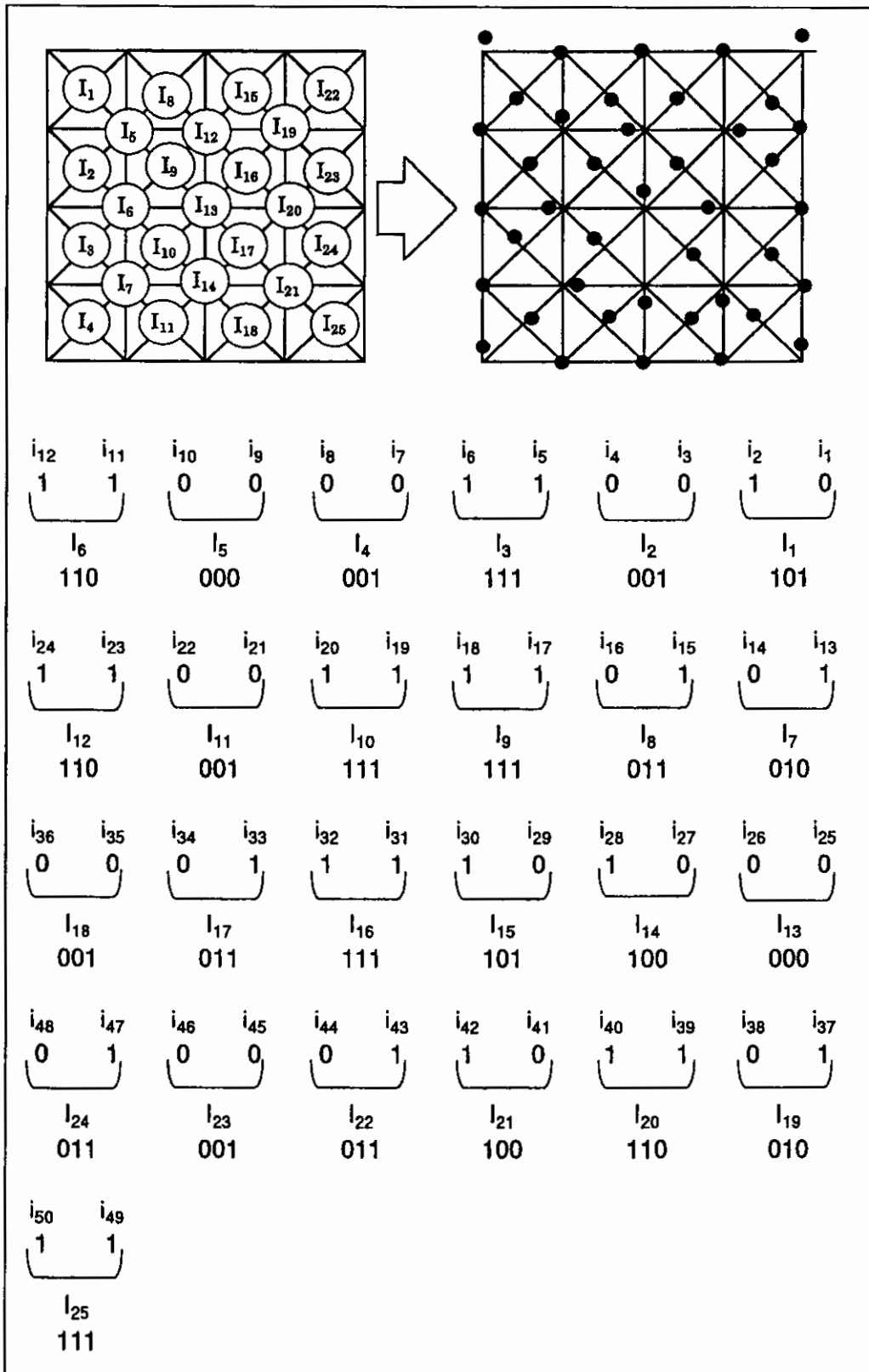


Fig. 8

K_{18}	K_{17}	K_{16}	K_{15}	K_{14}	K_{13}	K_{12}	K_{11}	K_{10}	K_9	K_8	K_7	K_6	K_5	K_4	K_3	K_2	K_1
100	010	110	000	110	100	100	000	100	000	000	010	000	100	100	000	110	100
R_{18}	R_{17}	R_{16}	R_{15}	R_{14}	R_{13}	R_{12}	R_{11}	R_{10}	R_9	R_8	R_7	R_6	R_5	R_4	R_3	R_2	R_1
101	001	001	101	110	100	010	001	011	111	011	000	110	100	101	111	011	001
l_{18}	l_{17}	l_{16}	l_{15}	l_{14}	l_{13}	l_{12}	l_{11}	l_{10}	l_9	l_8	l_7	l_6	l_5	l_4	l_3	l_2	l_1
001	011	111	101	100	000	110	001	111	111	011	010	110	000	001	111	001	101
※ The most significant two bits of $Kn(n=1 \text{ to } 25)$ is the true value. $ln(n=1 \text{ to } 25)$ consists of Security Table $Rn(n=1 \text{ to } 25)$ and Kn. The least significant one bit of Rn corresponds to that of the ln.																	
											K_{25}	K_{24}	K_{23}	K_{22}	K_{21}	K_{20}	K_{19}
											100	100	110	010	010	010	100
											R_{25}	R_{24}	R_{23}	R_{22}	R_{21}	R_{20}	R_{19}
											011	111	011	001	010	100	110
											l_{25}	l_{24}	l_{23}	l_{22}	l_{21}	l_{20}	l_{19}
											111	011	001	011	100	110	010

Fig. 9

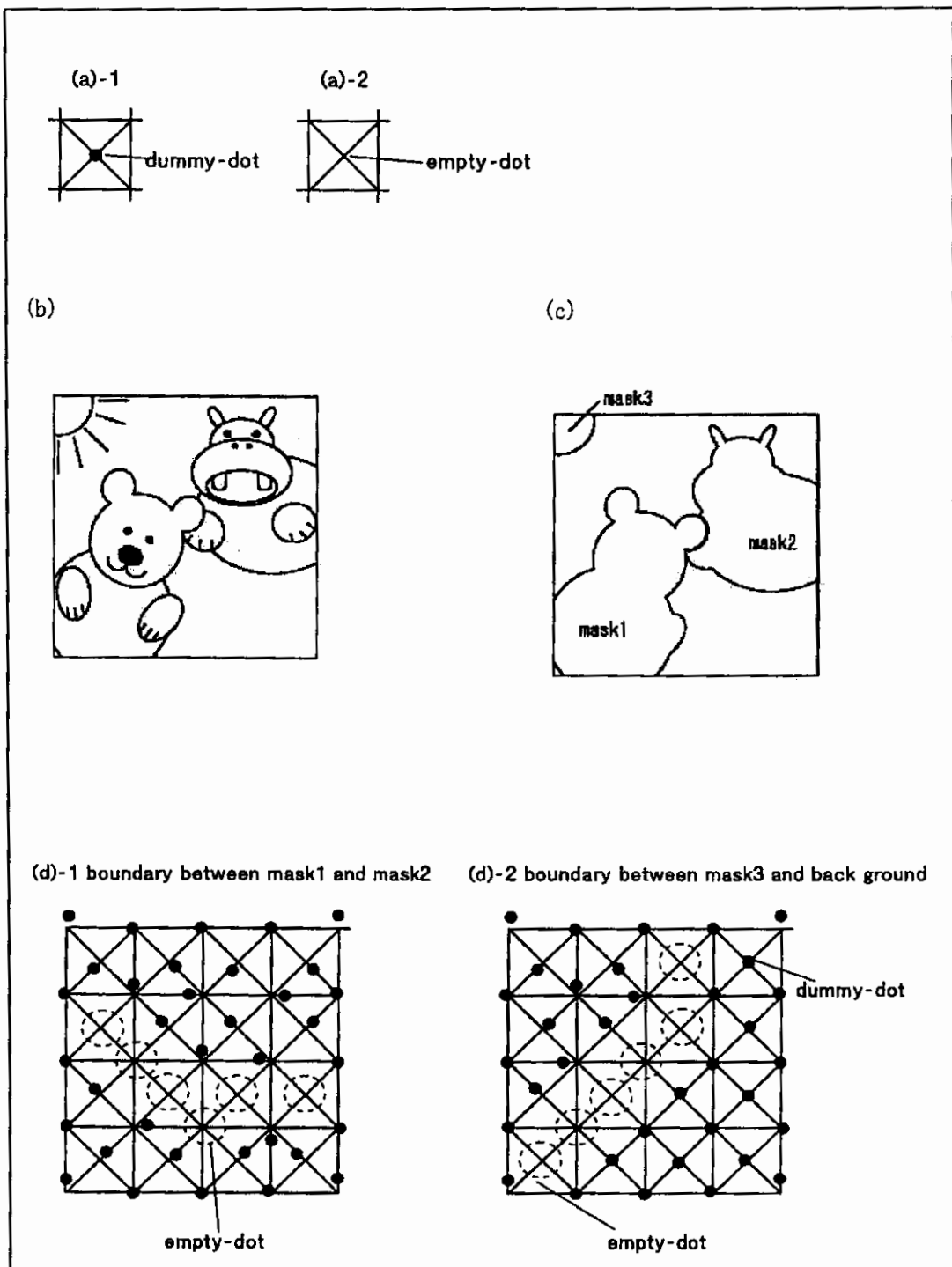


Fig. 10

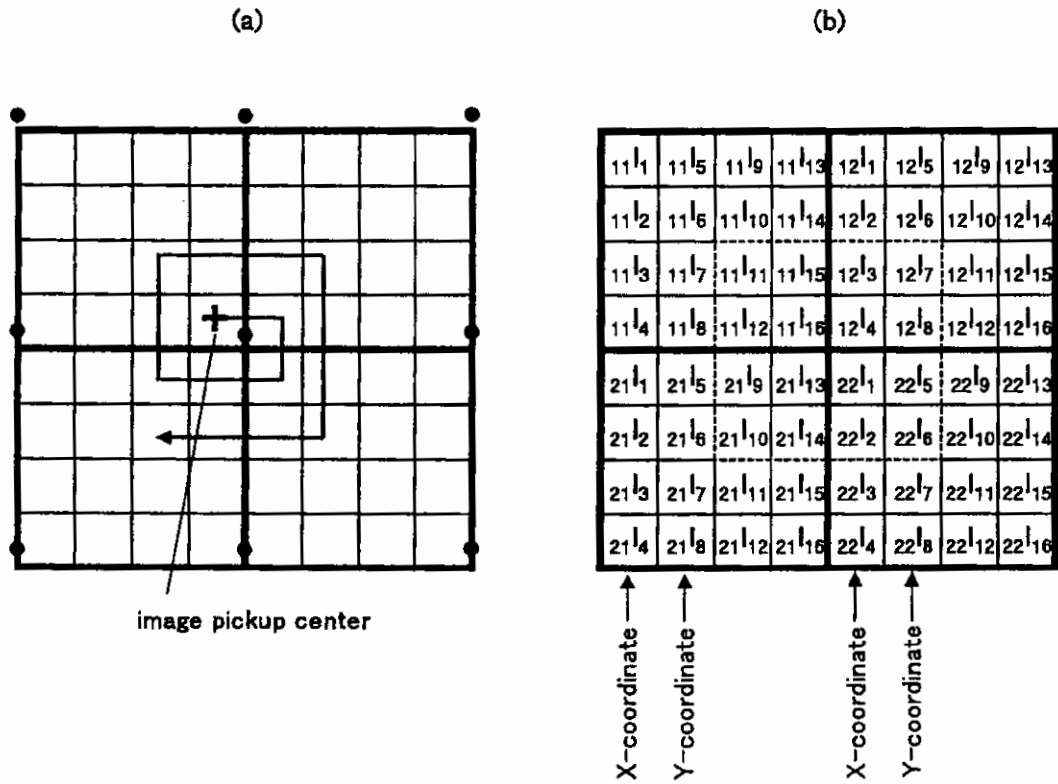


Fig. 11

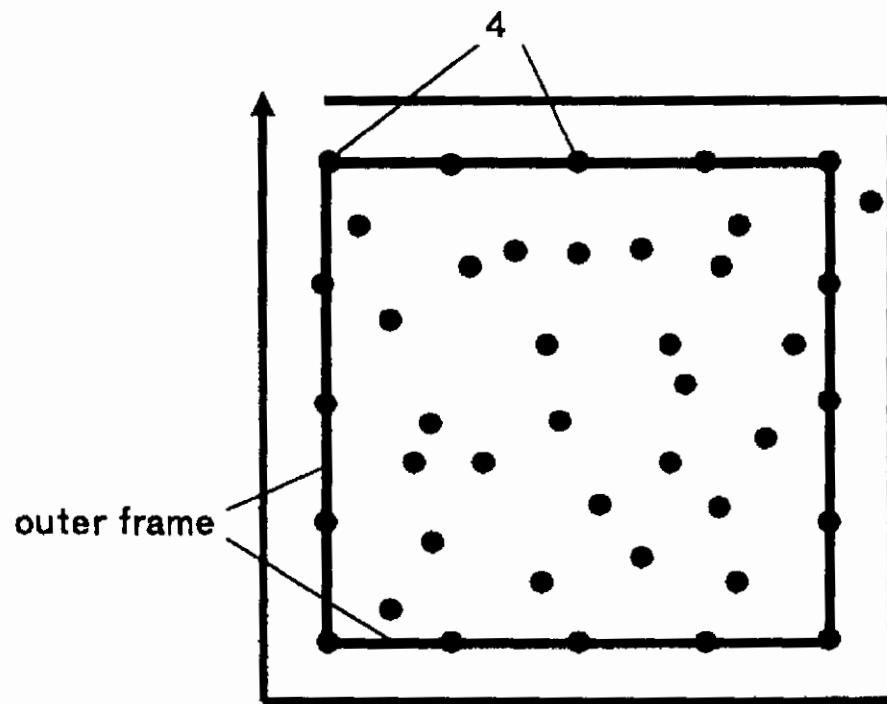


Fig. 12

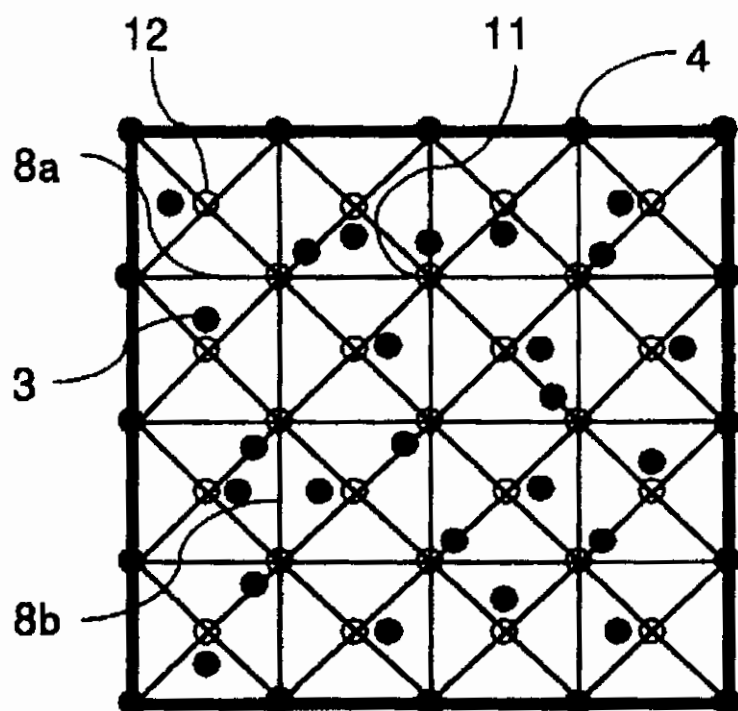


Fig. 13

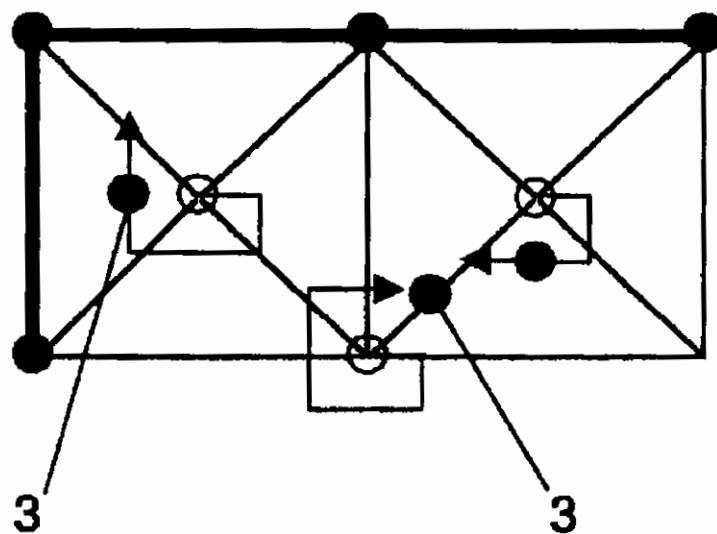


Fig. 14

