情報通信実験2 課題5

問題5-1

換字テーブル:

, Y

!, !

", "

#, #

$, $

%, %

&, &

', '

(, (

), )

\*, \*

+, +

,, H

-, -

., M

/, /

0, 0

1, 1

2, 2

3, 3

4, 4

5, 5

6, 6

7, 7

8, 8

9, 9

:, :

;, ;

<, <

=, =

>, >

?, ?

@, @

A, T

B, j

C, v

D, B

E, a

F, C

G, z

H, N

I, L

J, U

K, u

L, i

M, O

N, S

O, P

P, m

Q, l

R, q

S, V

T, e

U, h

V, I

W, .

X, s

Y,

Z, G

[, [

\, \

], ]

^, ^

\_, \_

`, `

a, W

b, E

c, g

d, y

e, f

f, k

g, t

h, c

i, p

j, A

k, R

l, d

m, Z

n, F

o, n

p, w

q, J

r, X

s, ,

t, K

u, o

v, x

w, b

x, D

y, r

z, Q

{, {

|, |

}, }

~, ~

, 

平文:

In our previous work, we proposed a biometric authentication method using a secure imaging system that was based on compressed sensing. In this approach, although we can acquire an encrypted vein image, the verification process requires the restoration of the raw finger-vein image. To address this issue, we propose an improved authentication method that we can verify alternate biometric features from which it is difficult to restore the original finger-vein image by introducing the permutation matrix for randomizing the object signal. Numerical simulations show that our method has favorable accuracy, although it exhibits a slightly degraded accuracy in comparison with that of the conventional method that uses a raw finger-vein image.

暗号文:

LFYnoXYwXfxpno,YbnXRHYbfYwXnwn,fyYWYEpnZfKXpgYWoKcfFKpgWKpnFYZfKcnyYo,pFtYWY,fgoXfYpZWtpFtY,r,KfZYKcWKYbW,YEW,fyYnFYgnZwXf,,fyY,fF,pFtMYLFYKcp,YWwwXnWgcHYWdKcnotcYbfYgWFYWgJopXfYWFYfFgXrwKfyYxfpFYpZWtfHYKcfYxfXpkpgWKpnFYwXngf,,YXfJopXf,YKcfYXf,KnXWKpnFYnkYKcfYXWbYkpFtfX-xfpFYpZWtfMYenYWyyXf,,YKcp,Yp,,ofHYbfYwXnwn,fYWFYpZwXnxfyYWoKcfFKpgWKpnFYZfKcnyYKcWKYbfYgWFYxfXpkrYWdKfXFWKfYEpnZfKXpgYkfWKoXf,YkXnZYbcpgcYpKYp,YypkkpgodKYKnYXf,KnXfYKcfYnXptpFWdYkpFtfX-xfpFYpZWtfYErYpFKXnyogpFtYKcfYwfXZoKWKpnFYZWKXpDYknXYXWFynZpQpFtYKcfYnEAfgKY,ptFWdMYSoZfXpgWdY,pZodWKpnF,Y,cnbYKcWKYnoXYZfKcnyYcW,YkWxnXWEdfYWggoXWgrHYWdKcnotcYpKYfDcpEpK,YWY,dptcKdrYyftXWyfyYWggoXWgrYpFYgnZwWXp,nFYbpKcYKcWKYnkYKcfYgnFxfFKpnFWdYZfKcnyYKcWKYo,f,YWYXWbYkpFtfX-xfpFYpZWtfMY

逆換字テーブル:

, Y

!, !

", "

#, #

$, $

%, %

&, &

', '

(, (

), )

\*, \*

+, +

,, s

-, -

., W

/, /

0, 0

1, 1

2, 2

3, 3

4, 4

5, 5

6, 6

7, 7

8, 8

9, 9

:, :

;, ;

<, <

=, =

>, >

?, ?

@, @

A, j

B, D

C, F

D, x

E, b

F, n

G, Z

H, ,

I, V

J, q

K, t

L, I

M, .

N, H

O, M

P, O

Q, z

R, k

S, N

T, A

U, J

V, S

W, a

X, r

Y,

Z, m

[, [

\, \

], ]

^, ^

\_, \_

`, `

a, E

b, w

c, h

d, l

e, T

f, e

g, c

h, U

i, L

j, B

k, f

l, Q

m, P

n, o

o, u

p, i

q, R

r, y

s, X

t, g

u, K

v, C

w, p

x, v

y, d

z, G

{, {

|, |

}, }

~, ~

, 

復号文:

In our previous work, we proposed a biometric authentication method using a secure imaging system that was based on compressed sensing. In this approach, although we can acquire an encrypted vein image, the verification process requires the restoration of the raw finger-vein image. To address this issue, we propose an improved authentication method that we can verify alternate biometric features from which it is difficult to restore the original finger-vein image by introducing the permutation matrix for randomizing the object signal. Numerical simulations show that our method has favorable accuracy, although it exhibits a slightly degraded accuracy in comparison with that of the conventional method that uses a raw finger-vein image.

問題5-2

問題点は使用する文字に偏りが見られること

問題5-3

平文:

Tokyo Institute of Technology is a national research university located in Greater Tokyo Area, Japan. Tokyo Tech is the largest institution for higher education in Japan dedicated to science and technology, and is generally considered to be one of the most prestigious universities in Japan. Tokyo Techs main campus is located at Ookayama on the boundary of Meguro and Ota, with its main entrance facing the Ookayama Station. Other campuses are located in Suzukakedai and Tamachi. Tokyo Tech is organized into six schools, within which there are over forty departments and research centers. Tokyo Tech enrolled four thousands seven hundreds thirty three undergraduates and one thousand four hundreds sixty four graduate students for two thousands fifteen to two thousand sixteen. It employs around one thousand and one hundred faculty members. The university has been ranked second in two thousands eleven in the field of Engineering by Scorenavi. In another ranking, Japanese prep school yawaijuku ranked Tokyo Tech as the fourth best, second or third best in former semester and first in latter semester university in Japan. According to QS World University Rankings, Tokyo Tech was ranked third in Japan and internationally ranked twentieth in the field of Engineering and Technology, and fifty first in Natural science in two thousands eleven. The university was ranked thirty first worldwide according to Global University ranking and fifty seventh in two thousands eleven according to QS World University Rankings. It was also ranked thirty first worldwide according to the Global University Ranking in two thousands eleven.

逆換字テーブル:

32, 118

33, 33

34, 34

35, 35

36, 36

37, 37

38, 38

39, 39

40, 40

41, 41

42, 42

43, 43

44, 69

45, 45

46, 102

47, 47

48, 48

49, 49

50, 50

51, 51

52, 52

53, 53

54, 54

55, 55

56, 56

57, 57

58, 58

59, 59

60, 60

61, 61

62, 62

63, 63

64, 64

65, 71

66, 44

67, 103

68, 117

69, 69

70, 99

71, 32

72, 72

73, 87

74, 105

75, 85

76, 120

77, 77

78, 78

79, 107

80, 104

81, 81

82, 121

83, 100

84, 101

85, 79

86, 106

87, 84

88, 77

89, 112

90, 116

91, 91

92, 92

93, 93

94, 94

95, 95

96, 96

97, 73

98, 81

99, 99

100, 100

101, 78

102, 65

103, 122

104, 108

105, 105

106, 97

107, 82

108, 108

109, 110

110, 110

111, 114

112, 109

113, 83

114, 46

115, 121

116, 111

117, 119

118, 115

119, 74

120, 120

121, 121

122, 98

123, 123

124, 124

125, 125

126, 126

127, 127

問題5-4

[0, 0]

[1, 1]

[2, 3]

[3, 2]

[4, 0]

[5, 0]

[6, 0]

[7, 1]

[8, 1]

[9, 0]

[10, 2]

[11, 1]

[12, 1]

[13, 0]

[14, 3]

[15, 2]

[16, 1]

[17, 2]

[18, 0]

[19, 0]

[20, 0]

[21, 1]

[22, 1]

[23, 1]

[24, 1]

[25, 3]

[26, 1]

[27, 2]

[28, 1]

[29, 1]

[30, 2]

[31, 0]

[32, 0]

[33, 0]

[34, 2]

[35, 0]

[36, 1]

[37, 1]

[38, 1]

[39, 0]

[40, 2]

[41, 3]

[42, 2]

[43, 2]

[44, 1]

[45, 0]

[46, 3]

[47, 0]

[48, 2]

[49, 2]

[50, 1]

[51, 1]

[52, 0]

[53, 0]

[54, 2]

[55, 0]

[56, 3]

[57, 2]

[58, 2]

[59, 0]

[60, 1]

[61, 1]

[62, 1]

[63, 3]

[64, 0]

[65, 2]

[66, 2]

[67, 1]

[68, 1]

[69, 2]

[70, 0]

[71, 1]

[72, 0]

[73, 0]

[74, 0]

[75, 1]

[76, 1]

[77, 2]

[78, 0]

[79, 2]

[80, 0]

[81, 0]

[82, 2]

[83, 1]

[84, 2]

[85, 2]

[86, 2]

[87, 4]

[88, 1]

[89, 1]

[90, 1]

[91, 2]

[92, 0]

[93, 2]

[94, 3]

[95, 4]

[96, 0]

[97, 1]

[98, 0]

[99, 2]

[100, 2]

[101, 2]

[102, 0]

[103, 1]

[104, 0]

[105, 0]

[106, 1]

[107, 1]

[108, 1]

[109, 2]

[110, 2]

[111, 0]

[112, 1]

[113, 3]

[114, 1]

[115, 2]

[116, 1]

[117, 0]

[118, 1]

[119, 3]

[120, 1]

[121, 2]

[122, 3]

[123, 1]

[124, 0]

[125, 1]

[126, 2]

[127, 0]

[128, 1]

[129, 1]

[130, 3]

[131, 4]

[132, 2]

[133, 2]

[134, 1]

[135, 1]

[136, 2]

[137, 1]

[138, 1]

[139, 0]

[140, 1]

[141, 2]

[142, 1]

[143, 4]

[144, 5]

[145, 1]

[146, 0]

[147, 2]

[148, 3]

[149, 2]

[150, 2]

[151, 1]

[152, 1]

[153, 3]

[154, 0]

[155, 3]

[156, 3]

[157, 1]

[158, 2]

[159, 1]

[160, 3]

[161, 5]

[162, 0]

[163, 2]

[164, 1]

[165, 0]

[166, 0]

[167, 2]

[168, 1]

[169, 1]

[170, 5]

[171, 4]

[172, 0]

[173, 0]

[174, 1]

[175, 1]

[176, 1]

[177, 1]

[178, 1]

[179, 1]

[180, 1]

[181, 3]

[182, 1]

[183, 1]

[184, 0]

[185, 0]

[186, 6]

[187, 1]

[188, 2]

[189, 0]

[190, 1]

[191, 2]

[192, 2]

[193, 0]

[194, 0]

[195, 2]

[196, 3]

[197, 2]

[198, 3]

[199, 0]

[200, 1]

[201, 2]

[202, 0]

[203, 0]

[204, 3]

[205, 1]

[206, 1]

[207, 0]

[208, 0]

[209, 0]

[210, 1]

[211, 3]

[212, 3]

[213, 1]

[214, 0]

[215, 3]

[216, 3]

[217, 0]

[218, 3]

[219, 3]

[220, 0]

[221, 1]

[222, 1]

[223, 0]

[224, 3]

[225, 1]

[226, 3]

[227, 0]

[228, 3]

[229, 2]

[230, 2]

[231, 3]

[232, 0]

[233, 1]

[234, 2]

[235, 2]

[236, 0]

[237, 1]

[238, 3]

[239, 4]

[240, 2]

[241, 2]

[242, 1]

[243, 2]

[244, 3]

[245, 1]

[246, 1]

[247, 1]

[248, 0]

[249, 0]

[250, 2]

[251, 0]

[252, 4]

[253, 3]

[254, 5]

[255, 0]

換字暗号に比べて、AESで暗号化すると、偏りが少ない。事実、換字暗号の時は最大値が二桁を優に越していたのに対し、AESの時は二桁に届くものはなかった。これにより、暗号に使われる文字の頻度から平文を推察される可能性が低い。

問題5-5

AES:

0 0 0 0 0 0 0 0 195 250 124 85 131 146 109 197 96 65 79 18 105 84 44 38 97 221 233 150 168 14 23 98 233 237 32 56 75 250 177 254 250 64 90 37 196 192 75 53 199 177 1 40 234 63 172 208 167 242 23 135 207 143 53 176 29 186 217 230 5 30 59 247 20 124 151 168 174 32 73 124 70 4 184 24 4 237 95 245 102 19 53 12 160 65 2 27 96 14 180 16 137 89 98 140 177 250 126 56 53 2 215 168 58 243 72 85 228 183 179 76 115 100 49 250 84 9 53 80 191 185 244 44 177 106 67 104 207 35 205 185 183 147 96 254 98 139 197 180 48 192 120 45 123 98 143 20 183 60 76 207 199 250 76 40 172 242 169 2 153 172 189 135 92 186 175 208 71 77 223 210 158 113 195 54 195 191 31 82 135 180 135 117 247 70 195 192 145 119 236 235 216 189 96 206 87 188 180 155 44 172 248 253 232 103 12 184 170 252 190 72 229 107 145 68 62 231 111 134 186 226 219 147 25 233 185 73 91 97 204 178 207 117 22 254 53 21 199 51 18 13 197 9 30 79 186 10 110 24 111 139 104 36 52 70 4 74 182 128 164 253 63 167 131 164 103 94 204 140 195 26 32 111 177 186 88 132 96 85 30 238 131 23 178 200 242 211 244 13 234 200 28 213 30 61 39 61 44 126 98 9 150 240 222 125 27 138 208 145 60 34 89 79 62 226 209 52 116 8 80 188 11 21 30 205 129 228 195 34 230 225 91 74 58 55 50 240 120 115 180 125 76 200 10 47 31 121 157 93 98 118 179 89 34 46 19 245 99 166 22 109 202 172 12 214 22 233 188 231 70 27 252 181 142 114 33 54 183 225 12 211 108 244 211 18 247 165 237 188 45 108 33 11 228 139 91 246 166 157 231 122 102 125 186 231 249 64 3 203 47 145 63 27 244 65 162 213 14 95 54 154 199 46 232 104 22 227 36 54 9 34 125 205 42 215 10 210 136 167 170 182 16 36 8 81 246 63 67 200 20 45 207 194 32 207 138 121 45 240 62 94 166 235 162 71 64 255 65 149 211 114 95 212 85 221 183 178 114 214 41 98 188 180 208 117 171 189 250 183 155 124 113 156 250 42 184 19 221 100 177 194 164 195 38 92 34 204 154 207 31 17 0 84 118 0 136 78 205 35 245 133 147 123 119 241 234 179 226 91 162 17 241 28 141 150 234 195 250 9 219 248 19 196 118 113 157 19 195 106 179 17 140 75 132 50 111 188 48 186 159 146 157 38 220 25 186 164 108 11 180 23 127 222 162 40 110 129 115 246 61 186 86 1 240 175 49 47 109 190 76 191 170 189 86 217 147 214 108 49 131 158 142 115 44 193 40 134 127 11 194 164 206 77 23 163 228 46 3 53 42 173 103 140 115 212 212 64 21 153 19 93 45 189 150 119 123 18 244 105 130 133 94 125 229 0 117 94 197 144 186 248 55 123 221 225 49 95 45 75 196 118 86 4 222 210 151 179 85 90 100 76 117 133 81 191 77 102 14 229 100 13 187 250 206 20 241 181 20 57 82 225 170 206 146 242 222 55 154 100 111 2 134 232 155 34 104 171 88 169 24 206 250 251 171 252 42 111 195 208 116 241 236 185 94 74 83 189 59 187 52 210 83 77 70 46 118 100 43 121 146 187 146 167 173 165 225 113 28 47 33 244 113 211 129 153 38 3 184 135

換字暗号:

32 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

見ての通り、AESでは変えたところも含め、多くの変更があるのに対して、換字暗号では変えたところが変わるだけである。したがって、安全性はAESの方が明らかに高い。

問題5-6

平文:

暗号鍵:

暗号文:

学生氏名:

暗号文:

復号鍵:

復号文:

学生氏名:

暗号文:

復号鍵:

復号文:

学生氏名:

暗号文:

復号鍵:

復号文: