**随堂测试题目**

学院 计算机与软件学院 专业 计算机科学与技术 姓名 郑雨婷 学号 2021150122 座号

( 密 封 线 内 不 答 题 )

……………………………………………………密………………………………………………封………………………………………线……………………………………线………………………………………

\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_

…

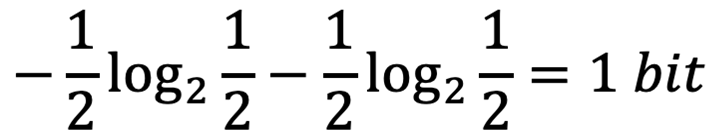
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 开/闭卷 | 开卷 | | A/B卷 | | | | |  |
| 课程编号 | 1500430001 | 课序号 | | 03/04 | 课程名称 | 专业英语 | 学分 | 2 |

命题人(签字) 审题人(签字) 2022年 12 月 22 日

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 题号 | 一 | 二 | 三 | 四 | 五 | 六 | 七 | 八 | 九 | 十 | 基本题总分 | 附加题 |
| 得分 |  |  |  |  |  |  |  |  |  |  |  |  |
| 评卷人 |  |  |  |  |  |  |  |  |  |  |  |  |

1. Introduce the basic idea of Shannon’s entropy and its connections with data compression. (20 points)

**Entropy is a measurement of the degree of randomness of energy in a system. The lower the entropy the more ordered and less random it is, and vice versa. In CS, entropy is all about probability. The entropy H(X) of a discrete random variable X is defined by**

**Toss coin: There are two probabilities in a fair coin. So if you get either head or tail, you will get 1 bit of information.. The size of file and image is usually represented by bits. When it comes to resolution, we find that same resolution has different entropy. So we can compress data by reducing entropy.**

1. Introduce the different methods to achieve network security. Briefly discuss their advantages and disadvantages. (20 points)

**There are key-based schemes and key-free schemes.**

**Inside key-based schemes, there are symmetric encryption and asymmetric encryption. In symmetric encryption, If use the same key, the message is not secure. So we can change the key for every next time(One-time pad). The safest is Quantum Key Distribution, Alice prepare states like |alive>, |dead>, |black> ,|white>.But does not tell Bob which hole to look at. Bob randomly pick which hole to check the state. Then Bob feedback his choices (blue or red). Asymmetric encryption using different key, there is a factorization,** **the result of the right side as a public key, and the parameters in the left produce a private key.**

**Inside Key-free schemes, there are Information theoretical security and Physical layer security. In information theoretical security, no key is needed, but it has leakage. Physical layer security uses artificial noise, Jamming and so on.**

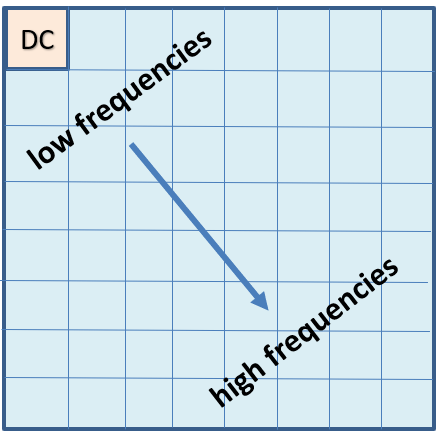
1. Describe the process of Joint Photographic Experts Group (JPEG) algorithm. Figures are necessary to assist the description. (20 points)

**The following picture shows four stages in image compression. In decoding, same process repeated inversely.**



**The first stage is color space conversion. The color model RGB is used for BMP images, and the color model YCrCb is used for JPEG images, so it is necessary to convert RGB color space image data to YCrCb color space data.**

**The second stage is block transform. Images are divided in blocks (8x8 pixels in JPEG) and each block is transformed to frequency domain. In the output block, upper left corner represents DC component (block average), upper left side low frequency components and lower right side high frequency components.**

****

**The third stage is quantization. For the human visual system, the low frequencies are the most important. Therefore, fine quantization is used for the low frequency part, and coarse quantization is used for the high frequency part.**

**The last stage is lossless coding. At first, Zic-zac scan is used. Zig-zag scan reads DCT coefficients in decreasing order of importance**

**The more important values (upper left) quantized with higher accuracy (smaller quantization steps). After quantization, a lot of zeros in the bottom right; can be coded efficiently with run-length coding. After quantization, coefficients need to be coded somehow.**

1. Please provide common organization, i.e., chapter setting, of a research paper and provide key points of each chapter. (30 points)

**1.Title:** **the title should be clear and interesting otherwise the reader will not continue reading.**

**2.Affiliations: authors’ names and affiliations.**

**3.Abstract: a one-page summary of the results.**

**4.Key Word: the professional terms that can best express the characteristics of the thesis theme from the selection of the thesis title, abstract and text.**

**5.Introduction: introduce your interpretation of the contest problem, your survey and discussion of the existing work relates to the problem, and your thoughts and approaches to solving the problem.**

**6.Related work:** **what results or progress have been made in the past.**

**7.Background and preliminaries: introduce the basic definitions, lemmas and other basic concepts required by the article, and carry out the deduction of relevant auxiliary conclusions**

**8.Method(s) and analysis: write what you did and how**

**9.Experiment:Include environment, settings, evaluation methods, results and discussions.**

**10.Conclusion: a summary of the full text. It should focus on summarizing the arguments of the full text.**

**11.Acknowledgement: Thank those who have helped and supported you in your research and writing.**

**12.References: Literature consulted during the writing of the thesis**

**13.Appendix: Raw data from tests, technical figures, graphs or tables and maps, charts or images.**

1. Describe the main idea of Hamming codes for reliable transmission. Use the famous parameter setting (N=7,K=4,d=3) as an example to assist your demonstration. (10 points)

**Hamming code is a kind of forward error correction. Firstly, the length of hamming code is 2^q-1. For example, when the parameter is the famous setting, it is 2^3-1=7. Then, use all non-zero number to form a matrix H. H comes to be as follow using the setting (N=7, K=4, d=3). A codeword must satisfy Hc^T=0, such as c=0000000, c=1110000 and so on. Hamming code can correct 1 error due to the equation Hc^T=0. For example, if you receive 0100100, compare it with the result of equation Hc^T=0 and find the minimum distance of them, then you get the answer 0100101. Hc^T tells you how to correct, which is called syndrome.**

