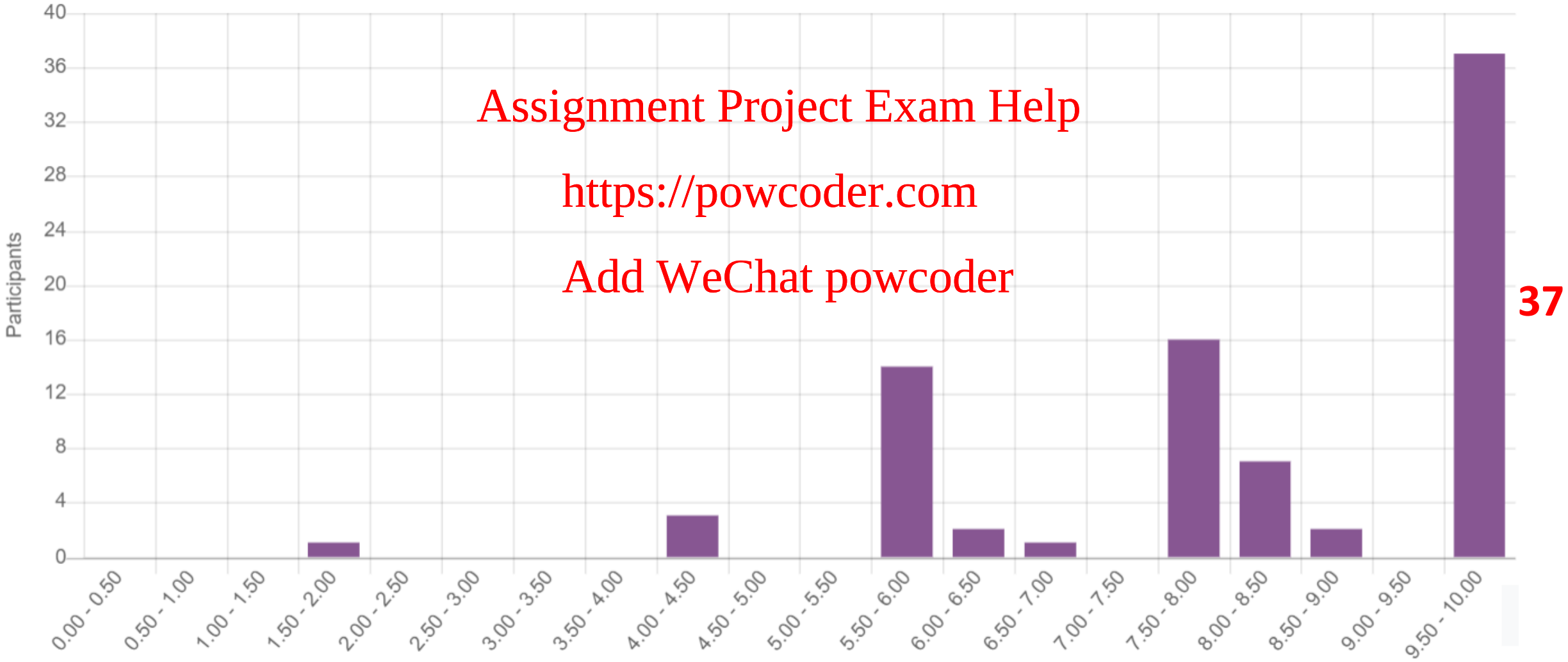
Quiz 5 - statistics

of participants: 83 / 100

average: 8.10 / 10

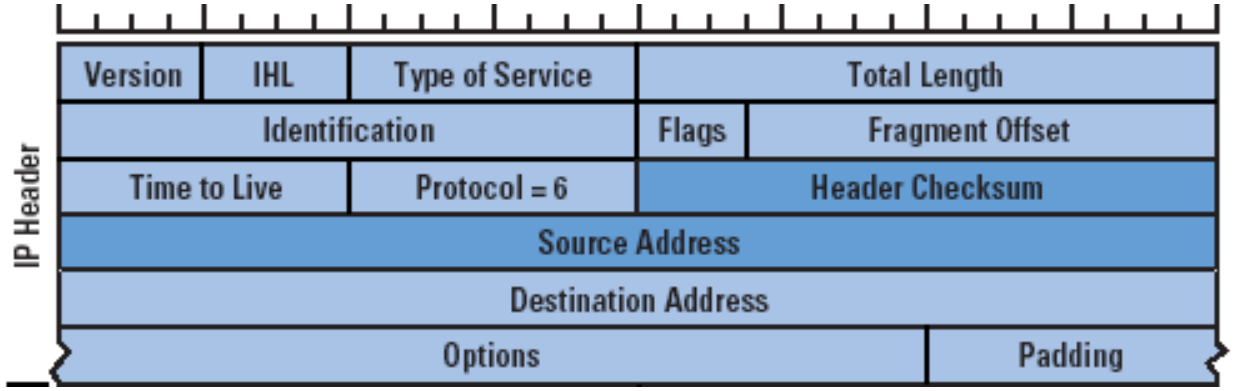


Alice is currently residing in New Zealand, and Bob is in Canada. They want to exchange secret messages (i.e., secret bits) using some form of network/datagram/packet steganography.

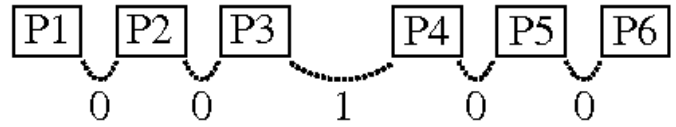
Which of the following forms of network steganography would be most suitable for them to deploy, in order to minimize the likelihood of any potential complications in the transmission and reception of secret bits?

1) hide the secret bits in 'version' field of transmitted IP packets
2) hide the secret bits in 'destination address' field of transmitted IP packets
3) hide the secret bits in 'total length' field of transmitted IP packets
4) hide the secret bits in inter-packet delay(s)

partial grade: 40%



Packets can be dropped or delayed significantly by intermediate routers, 'en route' to the destination.

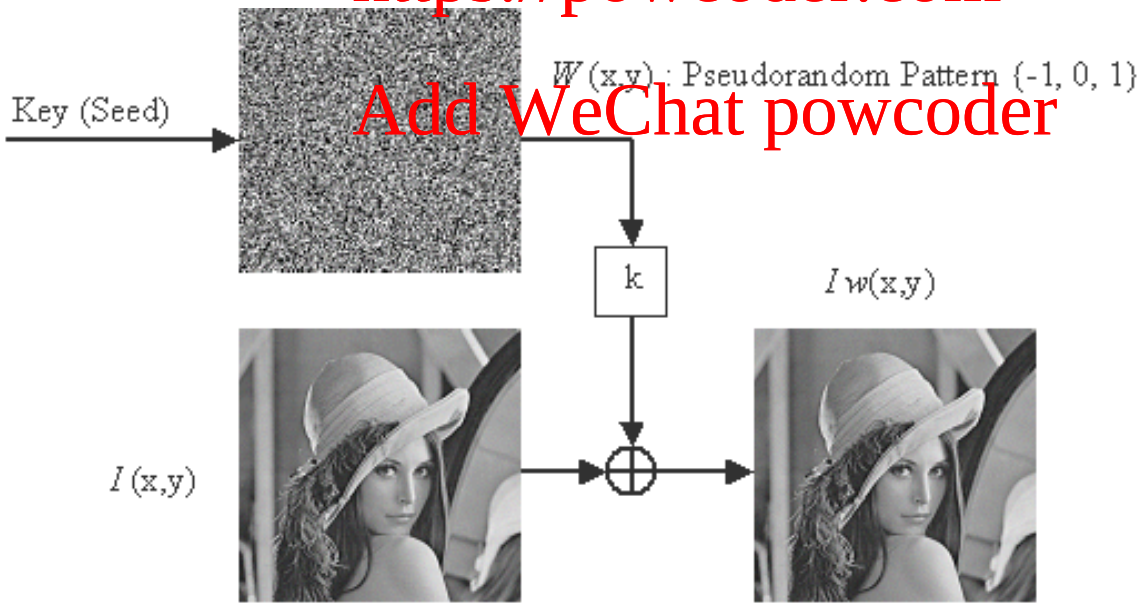


Entropy is a measure of unpredictability or randomness of information content. Which of the following do you expect to have higher entropy?

1) A digital image before a watermark is added to it.

2) A digital image after a watermark is added to it.

3) None of the above is correct. The entropy of an digital image before and after a watermark is added generally remains the same.

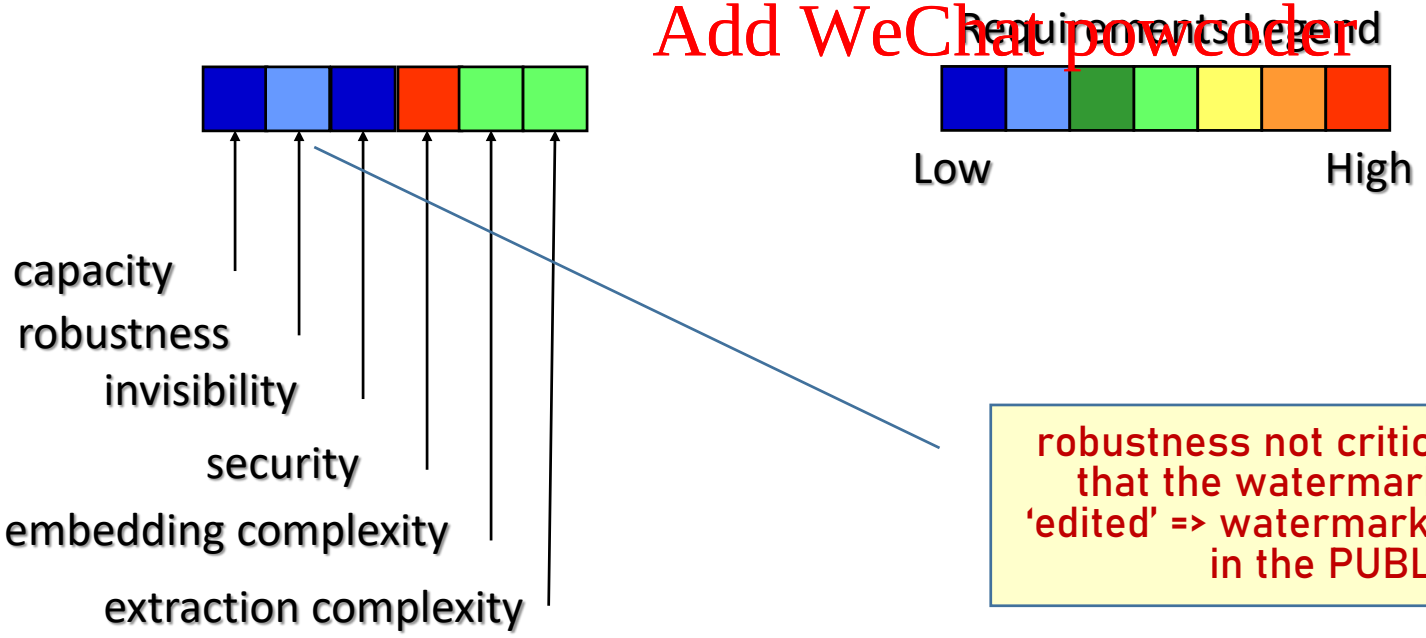


$$I_w(x,y) = I(x,y) + k*W(x,y)$$

Assume that for a particular watermarking application scenario, the requirements in terms of the six metrics discussed in class are as shown in the below figure.
What can you say about the given application scenario based on the provided information?

1) the application likely involves watermarking of real-time video
2) the application likely involves watermarking of high-quality still images
3) the application is a likely case of public watermarking
4) none of the above

partial grade: 40%



robustness not critical => not very likely that the watermarked object will be 'edited' => watermarked object likely NOT in the PUBLIC domain

Alice and Bob have exchanged a message that was encrypted using a well-known algorithm and a secret key of size 56 bits. Trudy has captured this message and wants to decrypt it. Through some form of social engineering, Trudy has learned that the first byte of the secret key used by Alice and Bob are all zeros.

If Trudy's computer can perform 2^{20} decryptions per second, how long will it take for Trudy to 'crack' (i.e., find) the key, in the worst case?

1) 2179.1 years
2) 1089.5 years
3) 26.5 years
4) 8.5 years

Key = 00000000 …..

56-8 = 48 bits

Search space = 2^{48} [keys]

Search time = 2^{48} [keys] / 2^{20} [keys/sec] = 2^{28} [sec]

Search time = 2^{28} [sec] / 60 / 60 / 24 / 365 = 8.5 [years]