Steganography Least Significant Method

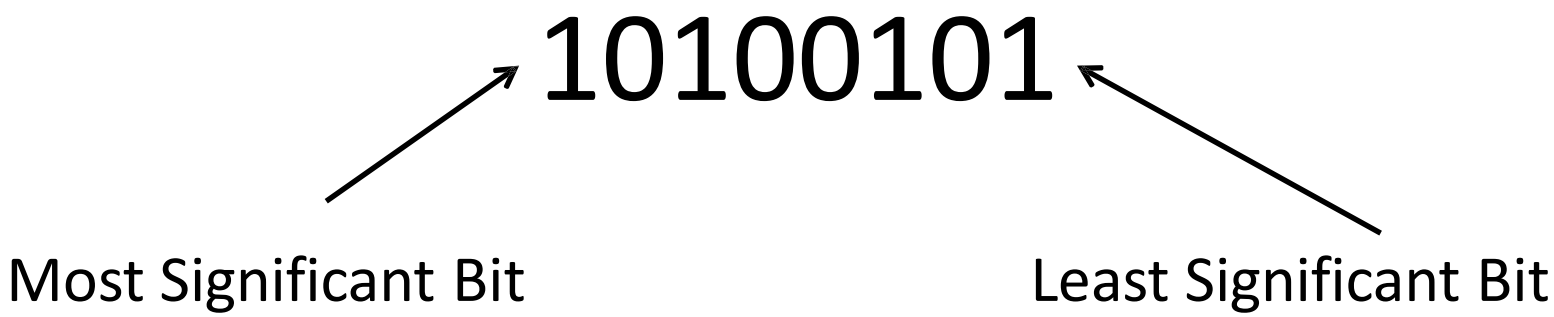
Dr Rosanne English

Digital Images – 24 Bit RGB

10101101 10110100 01011011

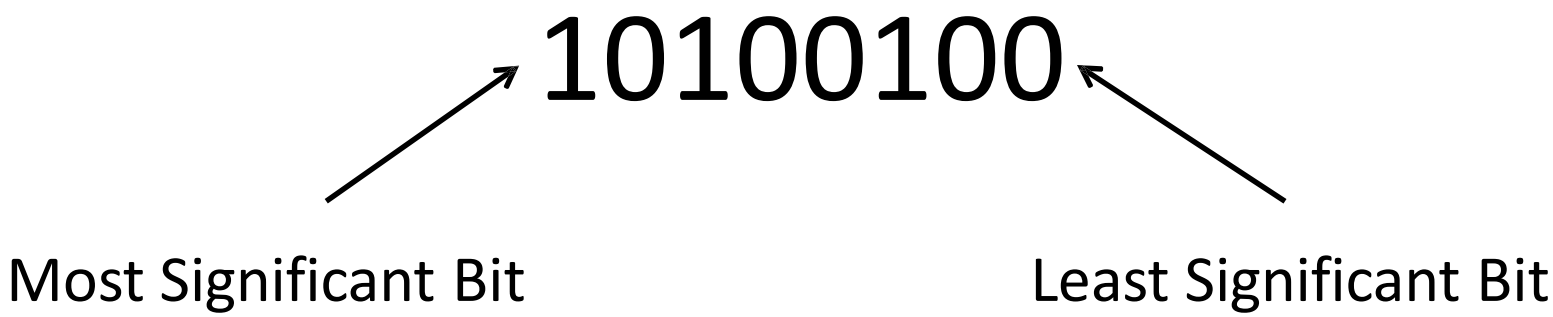
Red Value Green Value Blue Value

Significant Bits



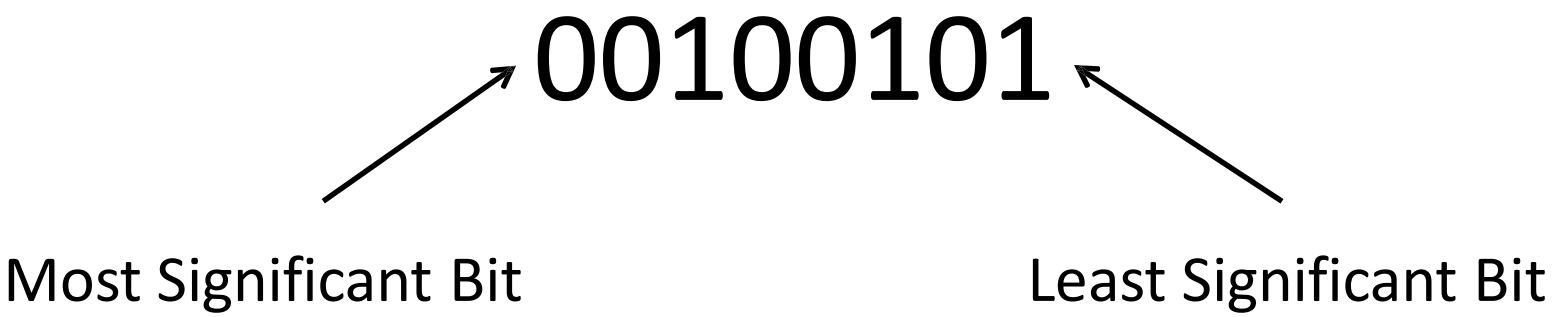
165

Significant Bits



164

Significant Bits Difference



37

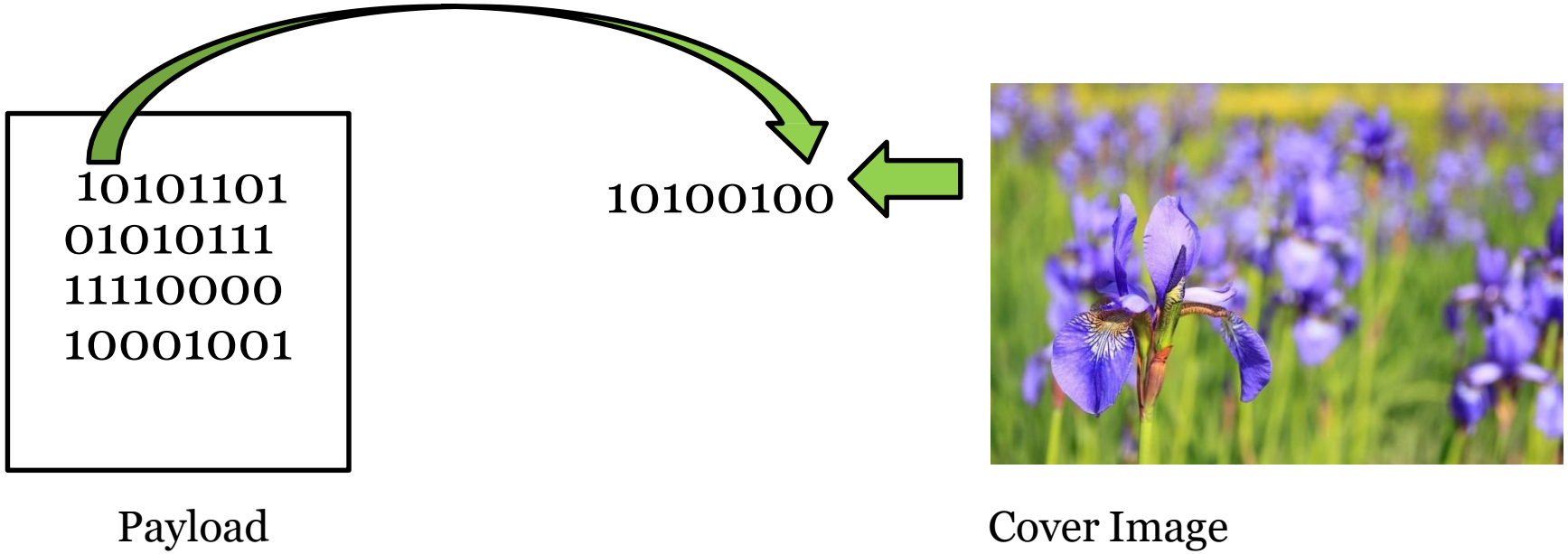
Pixel with R= 165 vs 164 vs 37

rgb(165, 0, 0)

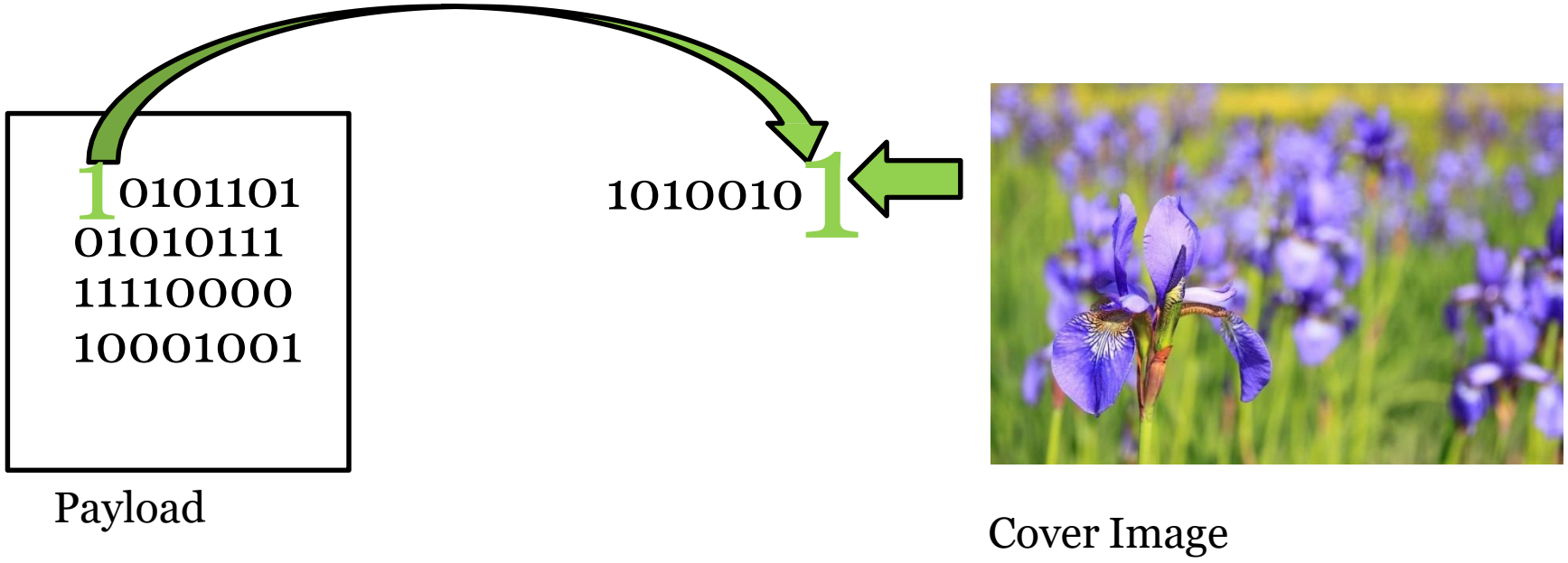
rgb(164, 0, 0)

rgb(37, 0, 0)

Least Significant Bits (LSB) Algorithm



Least Significant Bits (LSB) Algorithm



Cryptography and Randomness

- True random: entirely unpredictable events, such as lottery numbers
- Pseudo random: Statistically random sequence of numbers, but is repeatable with a seed value
- Cryptographically secure PRNG (Pseudorandom number generator): used in cryptography to provide sufficient security whilst remaining repeatable

e.g. `SecureRandom` in Java

Bit Manipulation in Java

`int lsb= byt & 0x1;`	get the lsb by performing bitwise and with 0x1
`byt &= ~ 0x1;`	change LSB to a 0 by bitwise and with the complement of 0x1
`byt |= 0x1;`	performs bitwise OR with 0X1 to change LSB to a 1
`byt << shiftVal;`	Shifts a byte to the left by int shiftVal
`byt >> shiftVal;`	shifts to the right by int shiftVal
`^`	performs exclusive OR