



Steganografia z poziomu teoretycznego i programowalnego

Łukasz Ogan, Wydział Matematyki i Informatyki UMK

Steganografia

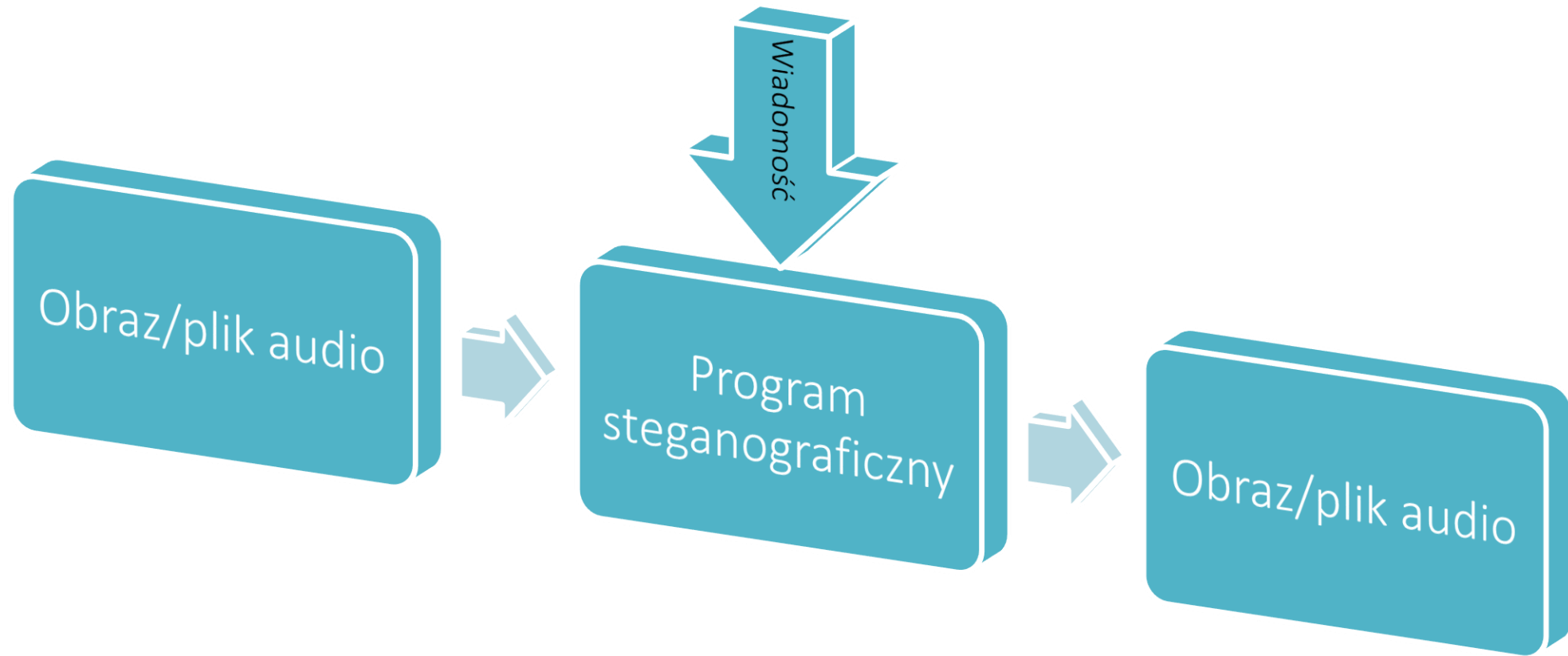
Pojęcie wywodzi się ze słów języka greckiego *steganos* (potajemny) i *grapho* (piszę)

Utajnianie informacji w innych informacjach

Dźwięk – wykorzystanie częstotliwości, których nie słyszy człowiek

Obraz – wykorzystanie nadmiarowych informacji o kolorze

Im lepsza jakość obrazu bądź dźwięku tym większa ilość nadmiarowych danych



NIEWIDOCZNOŚĆ = NIEWYKRYWALNOŚĆ

Nie tylko ukrycie informacji, ale również gwarancja niezauważalności zmian w nośniku.

Wady steganografii

Pojedyncza warstwa

Informacja może zostać odczyta przez każdego kto o niej wie i zna metodę ukrywania

Łatwe zniszczenie informacji

Ukrywane informacje muszą być dość małe

Podstawowe Pojęcia

Bit – (najmniejsza) jednostka logiczna stanowiąca wartościowanie 0 lub 1

Bajt - najmniejsza adresowalna jednostka informacji pamięci komputerowej, składająca się z 8 bitów, 1 bajt = jeden znak np. „z”

System binarny – system liczbowy, którego podstawą jest liczba 2. Do zapisu liczb potrzebne są tylko dwie cyfry: 0 i 1

$$1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 10$$

Najmniej znaczący BIT

Least significant bit, LSB – bit o najmniejszej wadze

$$11\ 1111 = 77$$

$$11\ 1110 = 76$$

$$01\ 1111 = 37$$



Tablica ascii

American Standard Code for
Information Interchange – 7 bitowa
tablica kodowa

Mapuje liczby z zakresu 0-127 na
podstawowe znaki

Każdy znak posiada 8 bitowy kod

Dec	Hex	Oct	Chr	Dec	Hex	Oct	HTML	Chr	Dec	Hex	Oct	HTML	Chr	Dec	Hex	Oct	HTML	Chr
0	0	000	NULL	32	20	040	 	Space	64	40	100	@	@	96	60	140	`	`
1	1	001	Start of Header	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	Start of Text	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	End of Text	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	End of Transmission	36	24	044	$	\$	68	44	104	D	D	100	64	144	d	d
5	5	005	Enquiry	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	Acknowledgment	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	Bell	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	Backspace	40	28	050	((72	48	110	H	H	104	68	150	h	h
9	9	011	Horizontal Tab	41	29	051))	73	49	111	I	I	105	69	151	i	i
10	A	012	Line feed	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	Vertical Tab	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	Form feed	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	Carriage return	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	Shift Out	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	Shift In	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	Data Link Escape	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	Device Control 1	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	Device Control 2	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	Device Control 3	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	Device Control 4	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	Negative Ack.	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	Synchronous idle	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	End of Trans. Block	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	Cancel	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	End of Medium	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	Substitute	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	Escape	59	3B	073	;	;	91	5B	133	[[123	7B	173	{	{
28	1C	034	File Separator	60	3C	074	<	<	92	5C	134	\	\	124	7C	174	|	
29	1D	035	Group Separator	61	3D	075	=	=	93	5D	135]	}	125	7D	175	}	}
30	1E	036	Record Separator	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	Unit Separator	63	3F	077	?	?	95	5F	137	_	_	127	7F	177		Del

asciicharstable.co

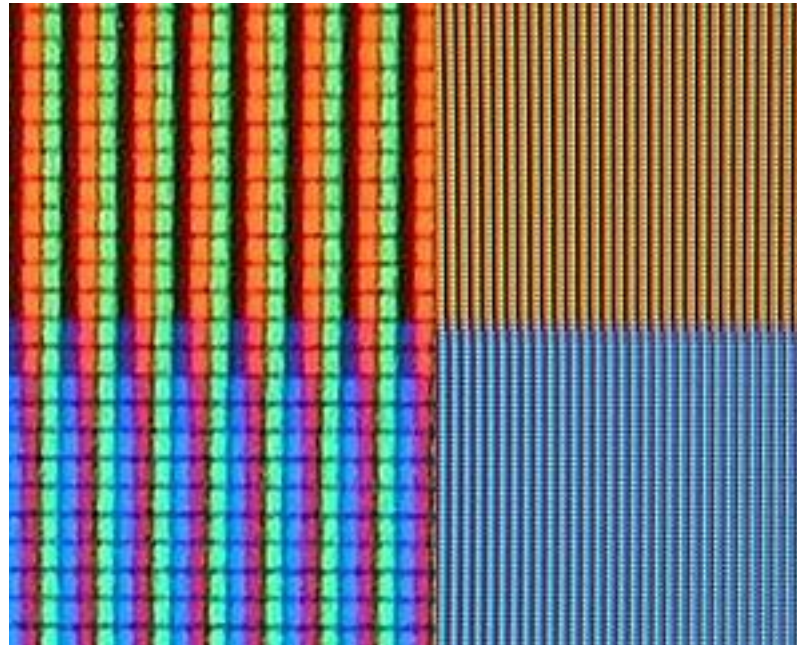
Dec	Hex	Oct	Chr	Dec	Hex	Oct	HTML	Chr	Dec	Hex	Oct	HTML	Chr	Dec	Hex	Oct	HTML	Chr
0	0	000	NULL	32	20	040	 	Space	64	40	100	@	@	96	60	140	`	`
1	1	001	Start of Header	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	Start of Text	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	End of Text	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	End of Transmission	36	24	044	$	\$	68	44	104	D	D	100	64	144	d	d
5	5	005	Enquiry	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	Acknowledgment	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	Bell	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	Backspace	40	28	050	((72	48	110	H	H	104	68	150	h	h
9	9	011	Horizontal Tab	41	29	051))	73	49	111	I	I	105	69	151	i	i
10	A	012	Line feed	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	Vertical Tab	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	Form feed	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	Carriage return	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	Shift Out	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	Shift In	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	Data Link Escape	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	Device Control 1	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	Device Control 2	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	Device Control 3	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	Device Control 4	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	Negative Ack.	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	Synchronous idle	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	End of Trans. Block	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	Cancel	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	End of Medium	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	Substitute	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	Escape	59	3B	073	;	;	91	5B	133	[[123	7B	173	{	{
28	1C	034	File Separator	60	3C	074	<	<	92	5C	134	\	\	124	7C	174	|	
29	1D	035	Group Separator	61	3D	075	=	=	93	5D	135]]	125	7D	175	}	}
30	1E	036	Record Separator	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	Unit Separator	63	3F	077	?	?	95	5F	137	_	_	127	7F	177		Del

RGB – Red Green Blue

Model barw oparty o zapisanie trzech kolorów w postaci liczbowej

24 bitowy RGB lub BRG – każdy piksel jest reprezentowany przez trzy 8 bitowe liczby naturalne, określające kolejno barwę czerwoną, zieloną i niebieską.

Widoczność pikseli



Dlaczego akurat RGB

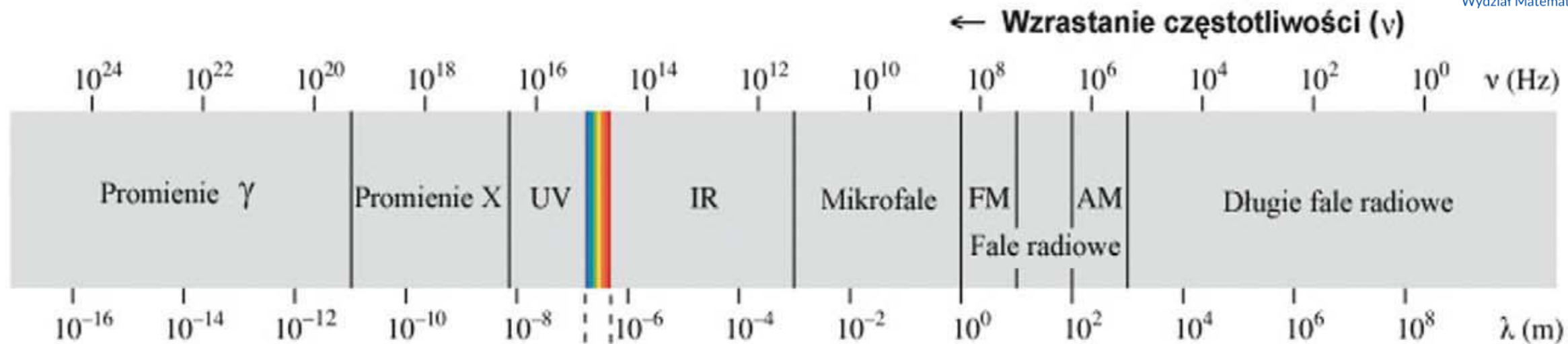
Wyświetlanie obrazu związane jest z budową ludzkiego oka

3 rodzaje czopków (światłoczułe receptory) reagują na światło widzialne o długości

564-580 nm – barwa czerwona

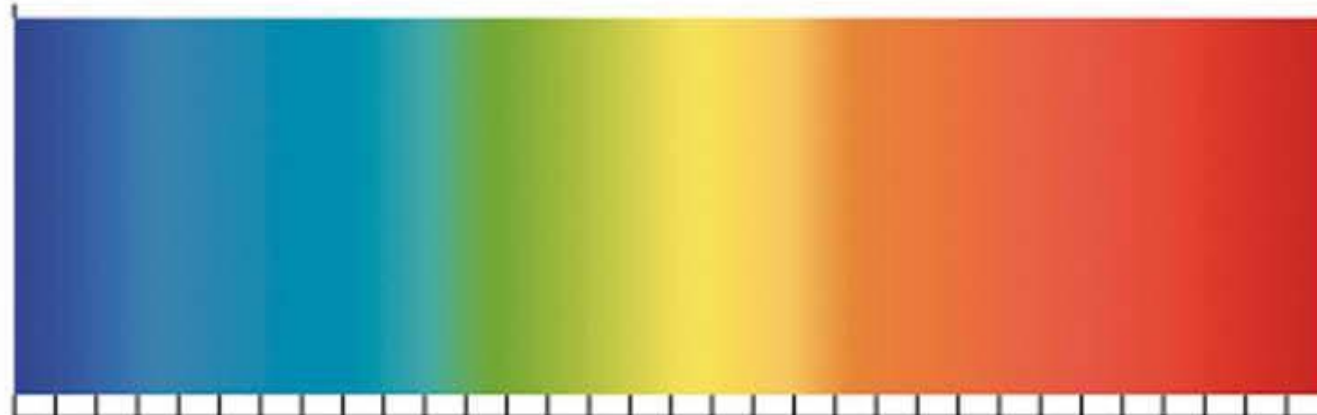
534-545 nm – barwa zielona

420-440 nm – barwa niebieska



Wzrastanie długości fali (λ) →

Widmo widzialne = Światło



400

500

600

700

Wzrastanie długości fali (λ) w nm →

Kolor biały

R

11111111

G

11111111

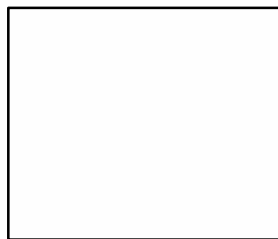
B

11111111

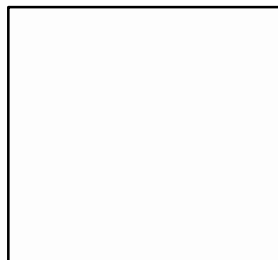
RGB(255, 255, 255)

Poziomy koloru białego

RGB(254, 254, 254)



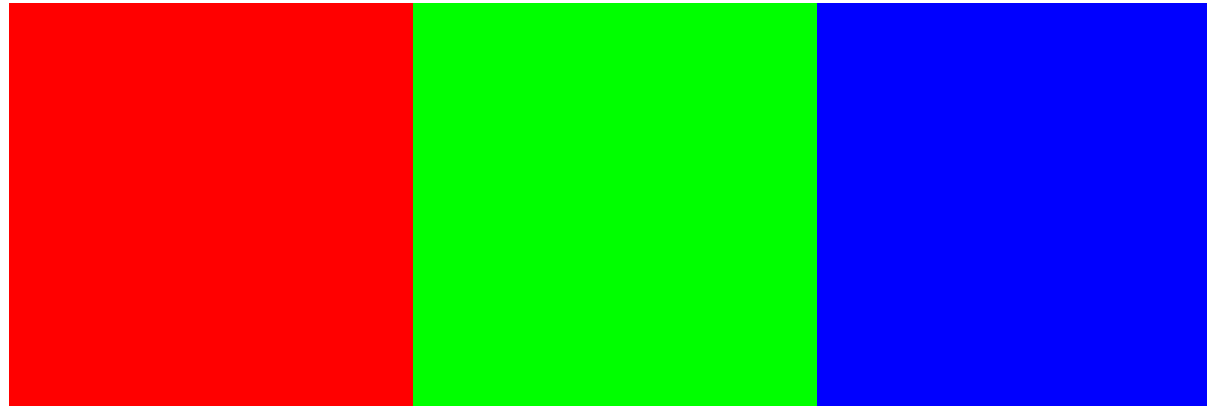
RGB(253, 253, 253, 253)



RGB (153, 253, 253)

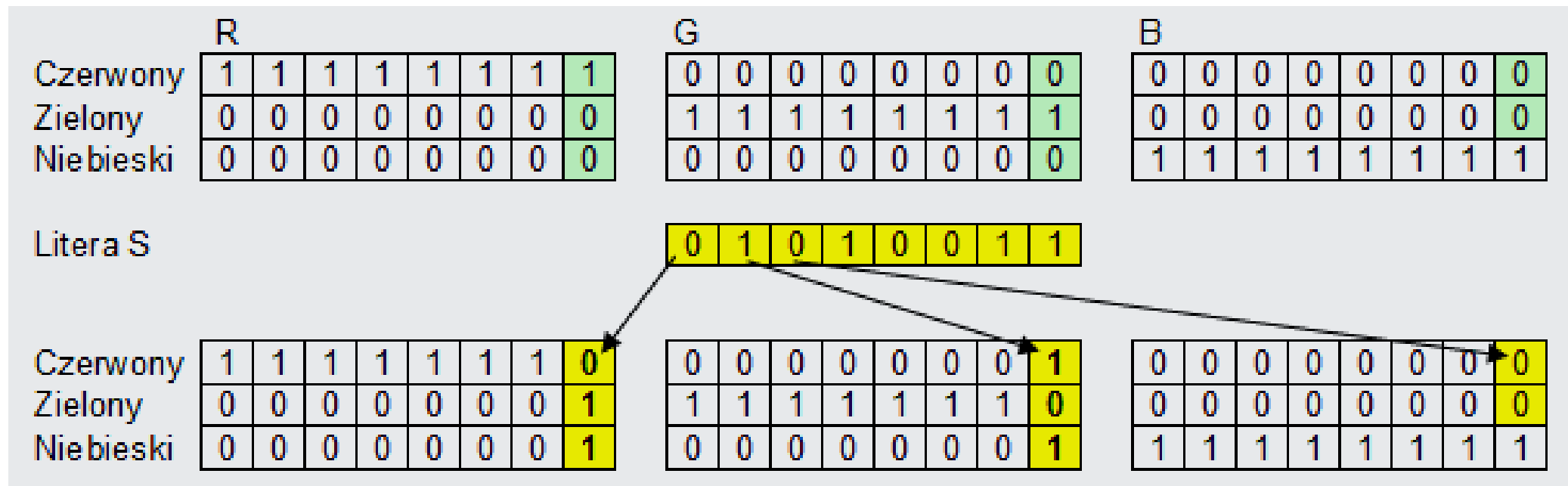


Ukrycie litery w obrazku

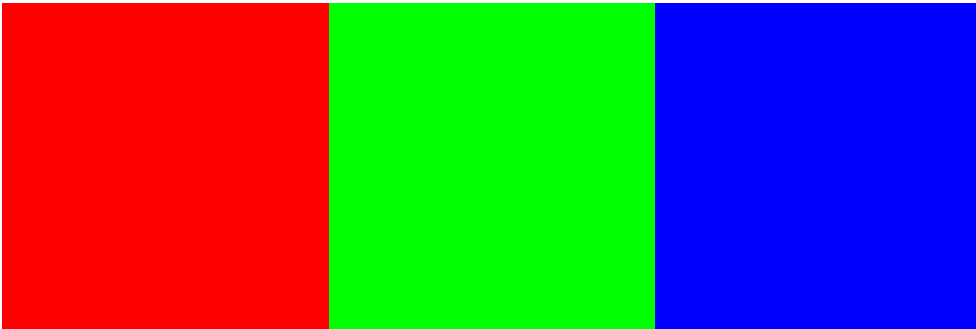


Ukrycie Litery S

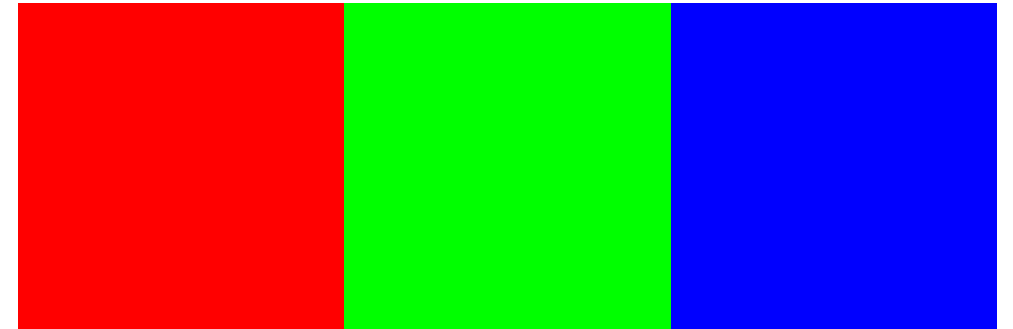
$S = 01010011$



Obrazek przed i po

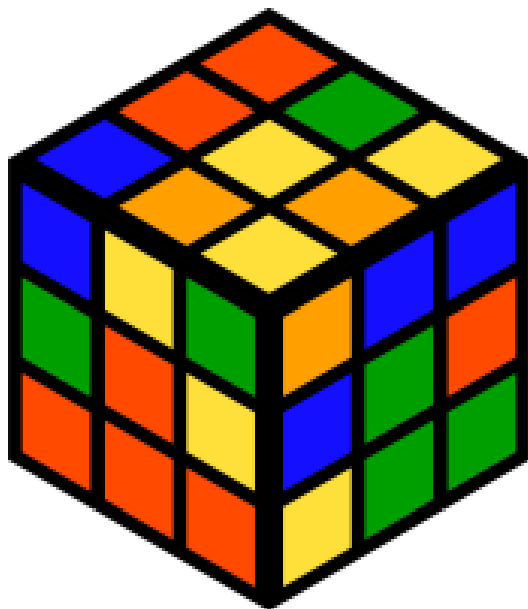


Obrazek przed ukryciem

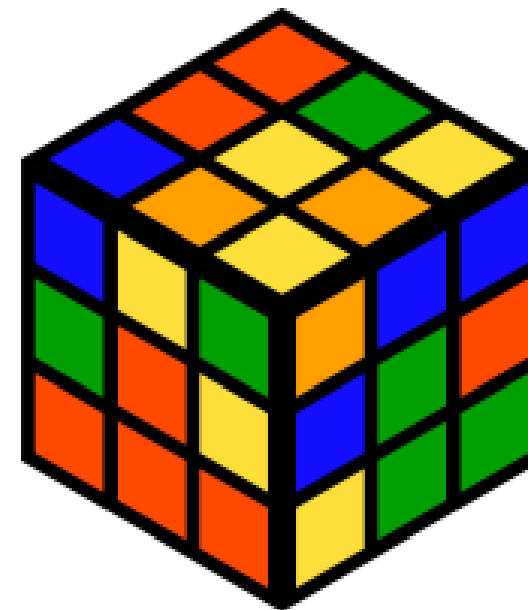


Obrazek po ukryciu

Większy fragment tekstu



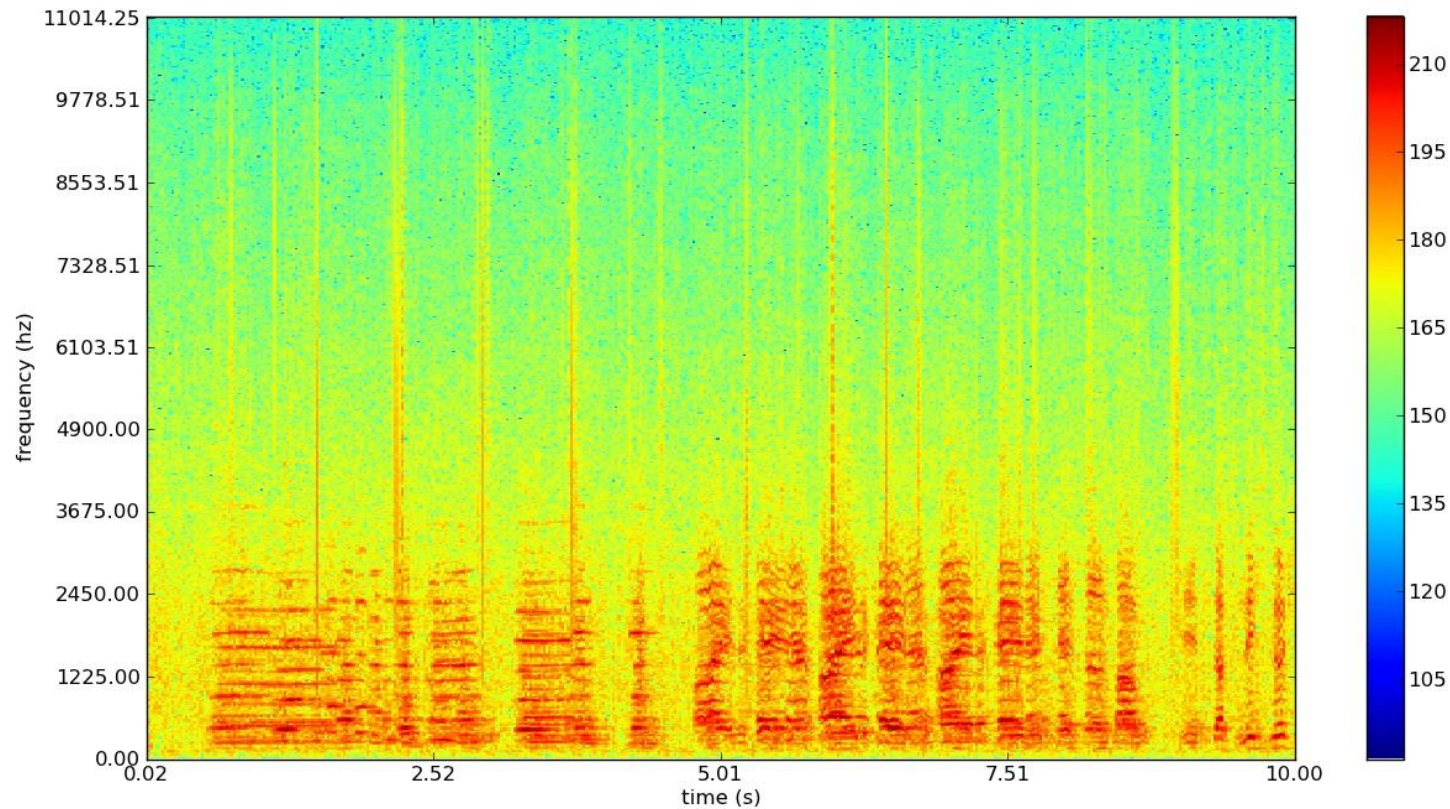
Rozmiar: 12,2 KB



Rozmiar: 14,9 KB

Ukryty tekst: to jest kawalek tekstu który chce ukryc poufna wiadomosc

Audio



Spektrogram - wykres widma amplitudowego sygnału

Ukrywanie informacji na częstotliwościach, których nie słyszy człowiek

Literatura

1. Gynael Coldwind, *Zrozumieć programowanie*
2. Volodymyr Mosorov, *Steganografia cyfrowa. Sztuka ukrywania informacji*
3. Marta Walenczykowska, *Analiza wybranych aplikacji stegograficznych*
4. Linux Magazine 62/2009, *Zabawy ze steganografią*
5. Cox, M. Miller, *Digital Watermarking and Steganography*, Morgan Kaufmann
6. Viswanathan V., *Information hiding in wave files through frequency domain*