

Positive Identification of LSB Image Steganography Using Cover Image Comparisons

Michael Pelosi

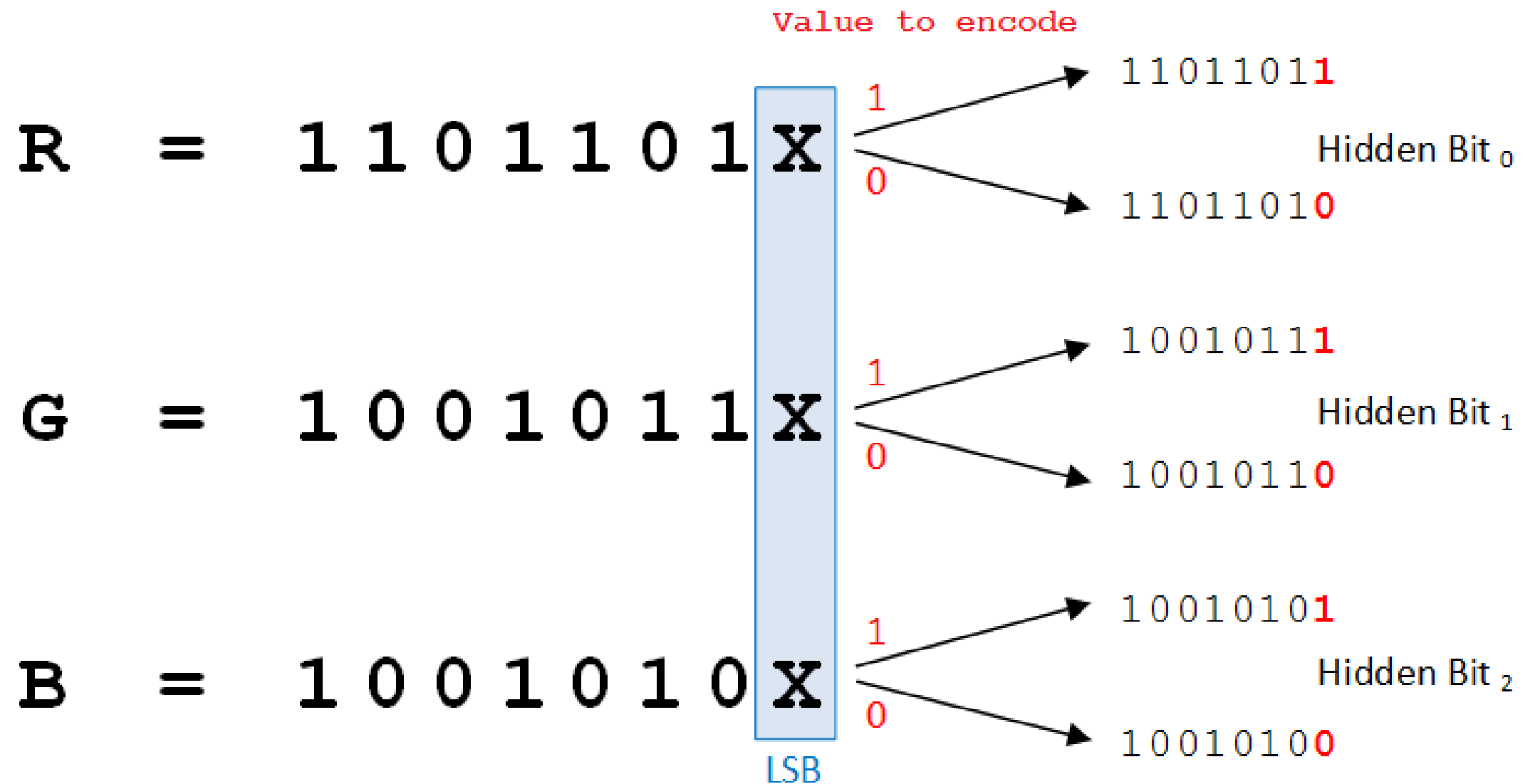
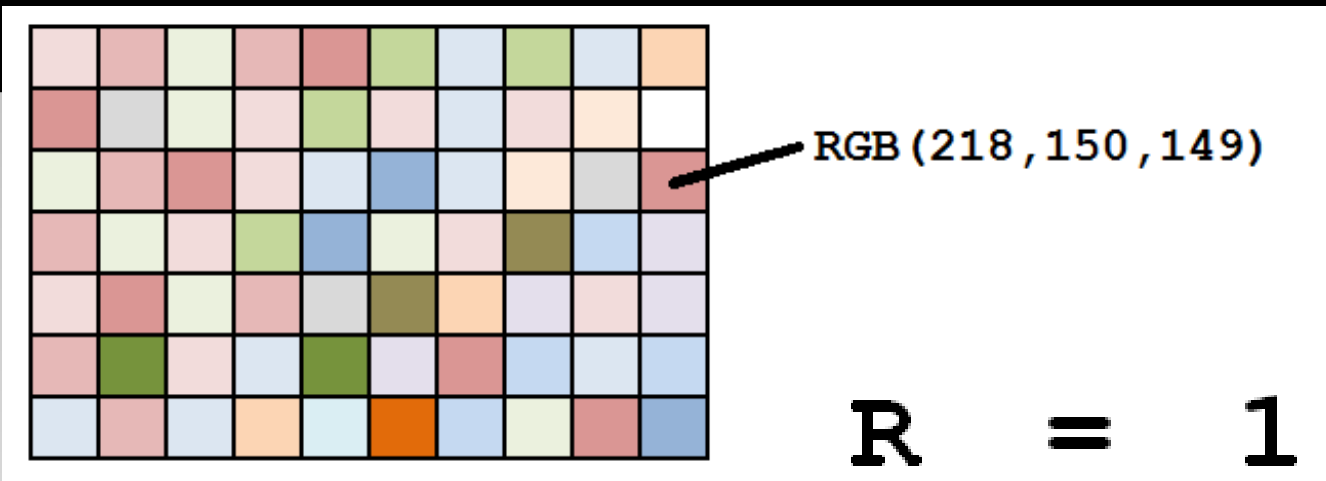
Texas A&M University
Texarkana, Texas



LSB Steganography

- The simplest and popular image steganographic method is the least significant bit (LSB) substitution.
- It embeds messages into cover image by replacing the least significant bits directly.
- The hiding capacity can be increased by using up to 4 least significant bits (one each for Red, Green, Blue, and Alpha color channels, respectively) in each pixel.
- It has a common weak point, the LSB value changes alter most images statistically to some extent.

LSB Steganography



Rise in the Usage of Steganography for Malware

- Microcin, alias Six Little Monkeys
- NetTraveler
- Zberp
- Enfal, and version with new loader called Zero.T
- Shamoon
- KinS
- ZeusVM
- Triton, alias Fibbit

Various Malware Using Steganography

- AdGholas – this malware hides malicious JavaScript in image, text, and HTML files
- Cerber – embeds malicious code in image files
- DNSChanger – uses PNG LSBs to hide malware AES encryption key
- Stegano – PNG formatted banner ads containing malicious code
- Stegoloadr (aka ‘Lurk’) – this malware uses both steganography and cryptography to conceal an encrypted URL to deliver later stage payloads
- Sundown – white PNG files are used to conceal exploit code or exfiltrate user data
- SyncCrypt – ransomware that hides part of its core code in image files
- TeslaCrypt – HTML comment tags in an HTTP 404 error page contain C2 server commands
- Vawtrak (aka ‘Neverquest’) – hides a URL in the LSBs of favicons in order to download a malicious payload
- VeryMal – malware targets macOS users with malicious javascript embedded in white bar
- Zbot – appends data to the end of a JPEG file containing hidden data
- ZeroT – Chinese malware that uses steganography to hide malware in an image of Britney Spears

Hiding Code Inside Images: How Malware Uses Steganography

https://www.sentinelone.com/blog/hiding-code-inside-images-malware-steganography/

Experiencing a Breach? 1-855-868-3733 Contact Cybersecurity Blog EN

SentinelOne[®] blog Platform Why SentinelOne? Services Partners Resources Company Get a Demo



Hiding Code Inside Images: How Malware Uses Steganography

July 4, 2019
by SentinelOne

f t in e m

CounterSteg v1.0

<http://199.175.52.196/CounterSteg/>

The screenshot displays the CounterSteg v1.0 application interface. The main window is titled "CounterSteg" and contains a menu bar with "New Analysis", "Window", "Help", "About", and "Exit". Below the menu bar, there are three tabs: "Browse", "Analysis", and "Image Comparison".

The "Image Comparison" window is active, showing a comparison between two images: "C:_CounterSteg\Images\clean05136.png" and "C:_CounterSteg\Images\gamma05136.png". The comparison results are displayed in a grid format with columns for "Complete", "All Bits", and bits 7 through 0. The rows represent different color channels: "All Colors", "Red", "Green", "Blue", and "Alpha".

	Complete	All Bits	7	6	5	4	3	2	1	0
All Colors										
		2,682,796-94%	490,331-17%	937,874-33%	1,799,521-63%	1,454,635-51%	1,959,440-68%	1,030,507-36%	1,407,420-49%	1,400,818-49%
Red										
		893,422-93%	203,178-21%	327,779-34%	598,604-63%	469,629-49%	668,063-70%	326,474-34%	466,489-49%	474,278-50%
Green										
		896,066-94%	180,017-19%	324,495-34%	600,163-63%	486,846-51%	664,385-69%	336,506-35%	467,857-49%	462,059-48%
Blue										
		893,308-93%	107,136-11%	285,600-30%	600,754-63%	498,160-52%	626,992-66%	367,527-38%	473,074-49%	464,481-49%
Alpha										
		-	-	-	-	-	-	-	-	-

An "About" dialog box is open in the foreground, displaying the following information:

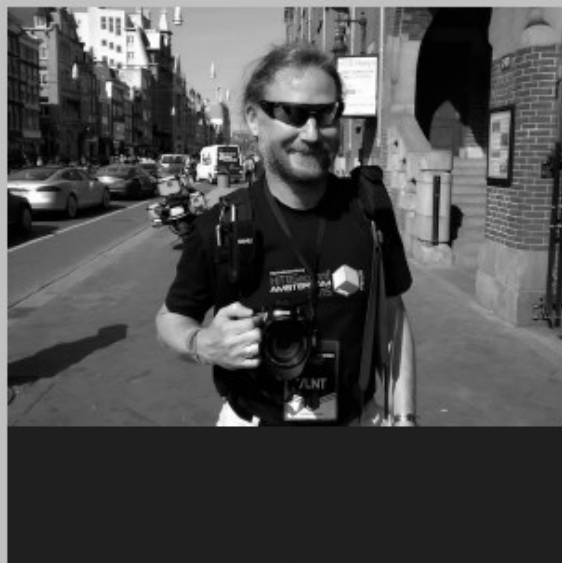
- CounterSteg**
- Counter Steganography Application
- <http://www.mauisolarsoftware.com/CounterSteg/>
- CounterSteg 1.0
- 01 JAN 2018
- OK

At the bottom of the main window, there is a "Image Analysis" window for "C:_CounterSteg\Images\clean05136.png", which shows a grid of image analysis results similar to the comparison window.

Search for images similar in the MSB bit color plane (85% or greater).

Browse

C:_CounterSteg\ImageTests\Kevin1.png



640 X 480 Pixels

Search Drive/Directory:

c: [SamsungSSD512GB_MAY2017]

- C:\
- CounterSteg
 - exifreader
 - Images
 - ImageTests
 - Paper
 - Setup
 - StegSoftware
 - Website

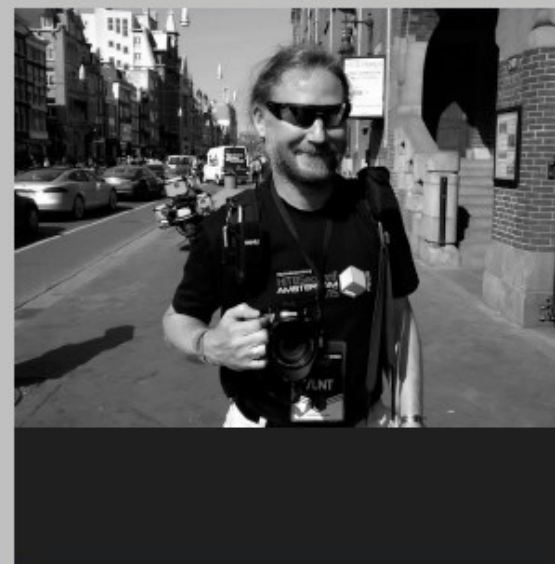
File Count: 0

Search

C:_CounterSteg\ImageTests\Kevin2.png

99.56%

C:_CounterSteg\ImageTests\Kevin2.png



640 X 480 Pixels

```
Filename: Kevin2.png
Directory: C:\\_CounterSteg\ImageTests\
FullFilePath: C:\\_CounterSteg\ImageTests\Kevin2.png
FileType: Unknown
VerMajor: 0
VerMinor: 0
VerRevision: 0
VerNotUsedVB: 0
FileSize: 270921
FileAttributes: 32
FileType: 0
CreationDate: 12/25/2017 9:40:11 PM
LastModifyTime: 12/25/2017 9:40:11 PM
LastAccessTime: 12/25/2017 9:40:11 PM
CompanyName:
FileDescription:
FileVersion:
InternalName:
LegalCopyright:
OriginalFileName:
ProductName:
ProductVersion:
Comment:
```

Search Count: 1

Places to find non-payload (also known as a “cover”) image:

- Suspect hard drive filesystems
- Suspect removable USB drives
- Suspect cameras and mobile devices
- Suspect CDs and DVDs
- Local email inboxes/outboxes
- Cloud email inboxes/outboxes
- Recent web search and browser histories
- Google image searches
- Network attached storage devices
- Employment computers and networks
- Recycle bins
- Deleted files removed from recycle bins
- Online photo galleries
- Personal and business associates' files as listed above

Results Using Various Steganographic Programs for Experimentation and Analysis

- **Steganography Online** – <http://stylesuxx.github.io/steganography/>
- **StegoShare** – <http://stegosshare.sourceforge.net/>
- **Geocaching Toolbox** – <https://www.geocachingtoolbox.com/index.php?page=steganography>
- **DevFarmSteganography** – <https://devfarm.it/steganography/>
- **f5stego.js** – <http://desudesutalk.github.io/f5stegojs/>
- **BitCrypt** – <http://bitcrypt.moshe-szweizer.com/>
- **OpenPuff** – http://embeddedsw.net/OpenPuff_Steganography_Home.html
- **OpenStego** – <https://www.openstego.com/index.html>
- **OTP-Steg** – <http://www.199.175.52.196.com/OTP-Steg/>

JFK Inauguration Speech

1,366 Words – 7,566 bytes – January 20, 1961

Vice President Johnson, Mr. Speaker, Mr. Chief Justice, President Eisenhower, Vice President Nixon, President Truman, Reverend Clergy, fellow citizens:

We observe today not a victory of party but a celebration of freedom--symbolizing an end as well as a beginning--signifying renewal as well as change. For I have sworn before you and Almighty God the same solemn oath our forbears prescribed nearly a century and three-quarters ago.

The world is very different now. For man holds in his mortal hands the power to abolish all forms of human poverty and all forms of human life. And yet the same revolutionary beliefs for which our forebears fought are still at issue around the globe--the belief that the rights of man come not from the generosity of the state but from the hand of God.

We dare not forget today that we are the heirs of that first revolution. Let the word go forth from this time and place, to friend and foe alike, that the torch has been passed to a new generation of Americans--born in this century, tempered by war, disciplined by a hard and bitter peace, proud of our ancient heritage--and unwilling to witness or permit the slow undoing of those human rights to which this nation has always been committed, and to which we are committed today at home and around the world.

Let every nation know, whether it wishes us well or ill, that we shall pay any price, bear any burden, meet any hardship, support any friend, oppose any foe to assure the survival and the success of liberty.

This much we pledge--and more.

To those old allies whose cultural and spiritual origins we share, we pledge the loyalty of faithful friends. United there is little we cannot do in a host of cooperative ventures. Divided there is little we can do--for we dare not meet a powerful challenge at odds and split asunder.

To those new states whom we welcome to the ranks of the free, we pledge our word that one form of colonial control shall not have passed away merely to be replaced by a far more iron tyranny. We shall not always expect to find them supporting our view. But we shall always hope to find them strongly supporting their own freedom--and to remember that, in the past, those who foolishly sought power by riding the back of the tiger ended up inside.

To those people in the huts and villages of half the globe struggling to break the bonds of mass misery, we pledge our best efforts to help them help themselves, for whatever period is required--not because the communists may be doing it, not because we seek their votes, but because it is right. If a free society cannot help the many who are poor, it cannot save the few who are rich.

To our sister republics south of our border, we offer a special pledge--to convert our good words into good deeds--in a new alliance for progress--to assist free men and free governments in casting off the chains of poverty. But this peaceful revolution of hope cannot become the prey of hostile powers. Let all our neighbors know that we shall join with them to oppose aggression or subversion anywhere in the Americas. And let every other power know that this Hemisphere intends to remain the master of its own house.

To that world assembly of sovereign states, the United Nations, our last best hope in an age where the instruments of war have far outpaced the instruments of peace, we renew our pledge of support--to prevent it from becoming merely a forum for invective--to strengthen its shield of the new and the weak--and to enlarge the area in which its writ may run.

Finally, to those nations who would make themselves our adversary, we offer not a pledge but a request: that both sides begin anew the quest for peace, before the dark powers of destruction unleashed by science engulf all humanity in planned or accidental self-destruction.

We dare not tempt them with weakness. For only when our arms are sufficient beyond doubt can we be certain beyond doubt that they will never be employed.

But neither can two great and powerful groups of nations take comfort from our present course--both sides overburdened by the cost of modern weapons, both rightly alarmed by the steady spread of the deadly atom, yet both racing to alter that uncertain balance of terror that stays the hand of mankind's final war.

So let us begin anew--remembering on both sides that civility is not a sign of weakness, and sincerity is always subject to proof. Let us never negotiate out of fear. But let us never fear to negotiate.

Let both sides explore what problems unite us instead of belaboring those problems which divide us.

Let both sides, for the first time, formulate serious and precise proposals for the inspection and control of arms--and bring the absolute power to destroy other nations under the absolute control of all nations.

Let both sides seek to invoke the wonders of science instead of its terrors. Together let us explore the stars, conquer the deserts, eradicate disease, tap the ocean depths and encourage the arts and commerce.

Let both sides unite to heed in all corners of the earth the command of Isaiah--to "undo the heavy burdens . . . (and) let the oppressed go free."

And if a beachhead of cooperation may push back the jungle of suspicion, let both sides join in creating a new endeavor, not a new balance of power, but a new world of law, where the strong are just and the weak secure and the peace preserved. All this will not be finished in the first one hundred days. Nor will it be finished in the first one thousand days, nor in the life of this Administration, nor even perhaps in our lifetime on this planet. But let us begin.

In your hands, my fellow citizens, more than mine, will rest the final success or failure of our course. Since this country was founded, each generation of Americans has been summoned to give testimony to its national loyalty. The graves of young Americans who answered the call to service surround the globe.

Now the trumpet summons us again--not as a call to bear arms, though arms we need--not as a call to battle, though embattled we are-- but a call to bear the burden of a long twilight struggle, year in and year out, "rejoicing in hope, patient in tribulation"--a struggle against the common enemies of man: tyranny, poverty, disease and war itself.

Can we forge against these enemies a grand and global alliance, North and South, East and West, that can assure a more fruitful life for all mankind? Will you join in that historic effort?

In the long history of the world, only a few generations have been granted the role of defending freedom in its hour of maximum danger. I do not shrink from this responsibility--I welcome it. I do not believe that any of us would exchange places with any other people or any other generation. The energy, the faith, the devotion which we bring to this endeavor will light our country and all who serve it--and the glow from that fire can truly light the world.

And so, my fellow Americans: ask not what your country can do for you--ask what you can do for your country.

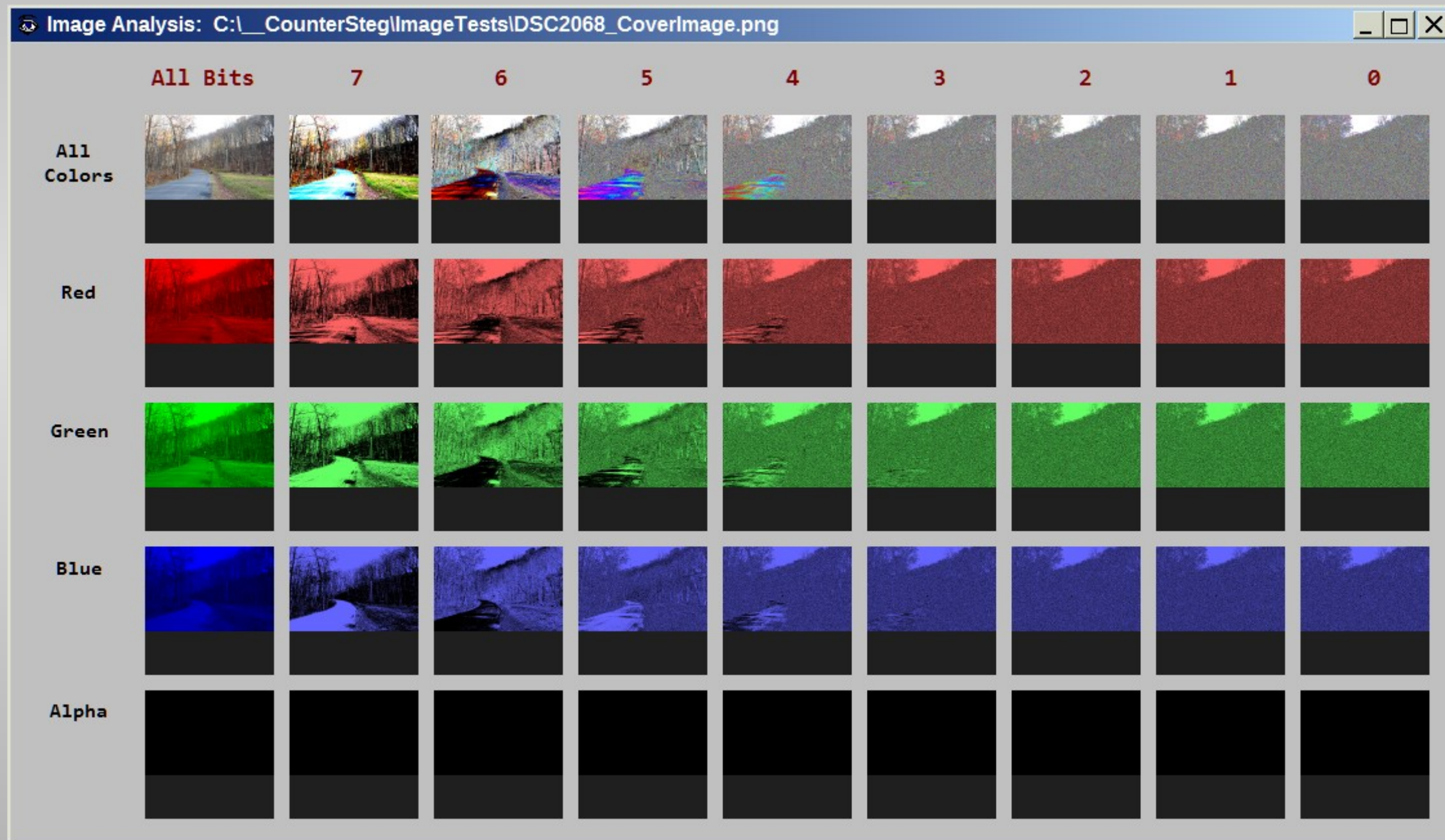
My fellow citizens of the world: ask not what America will do for you, but what together we can do for the freedom of man.

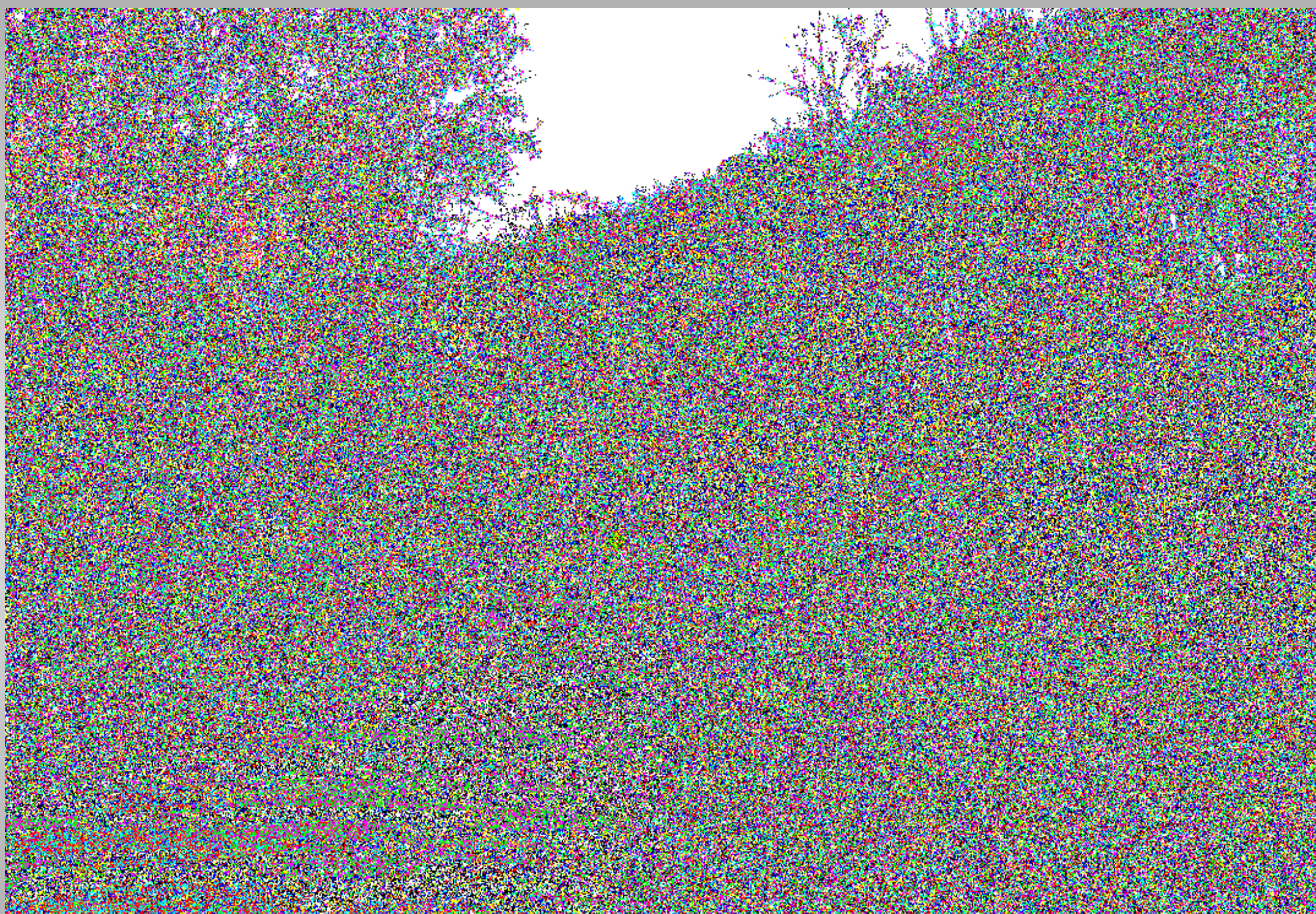
Finally, whether you are citizens of America or citizens of the world, ask of us here the same high standards of strength and sacrifice which we ask of you. With a good conscience our only sure reward, with history the final judge of our deeds, let us go forth to lead the land we love, asking His blessing and His help, but knowing that here on earth God's work must truly be our own.

Cover image taken with Nikon D90

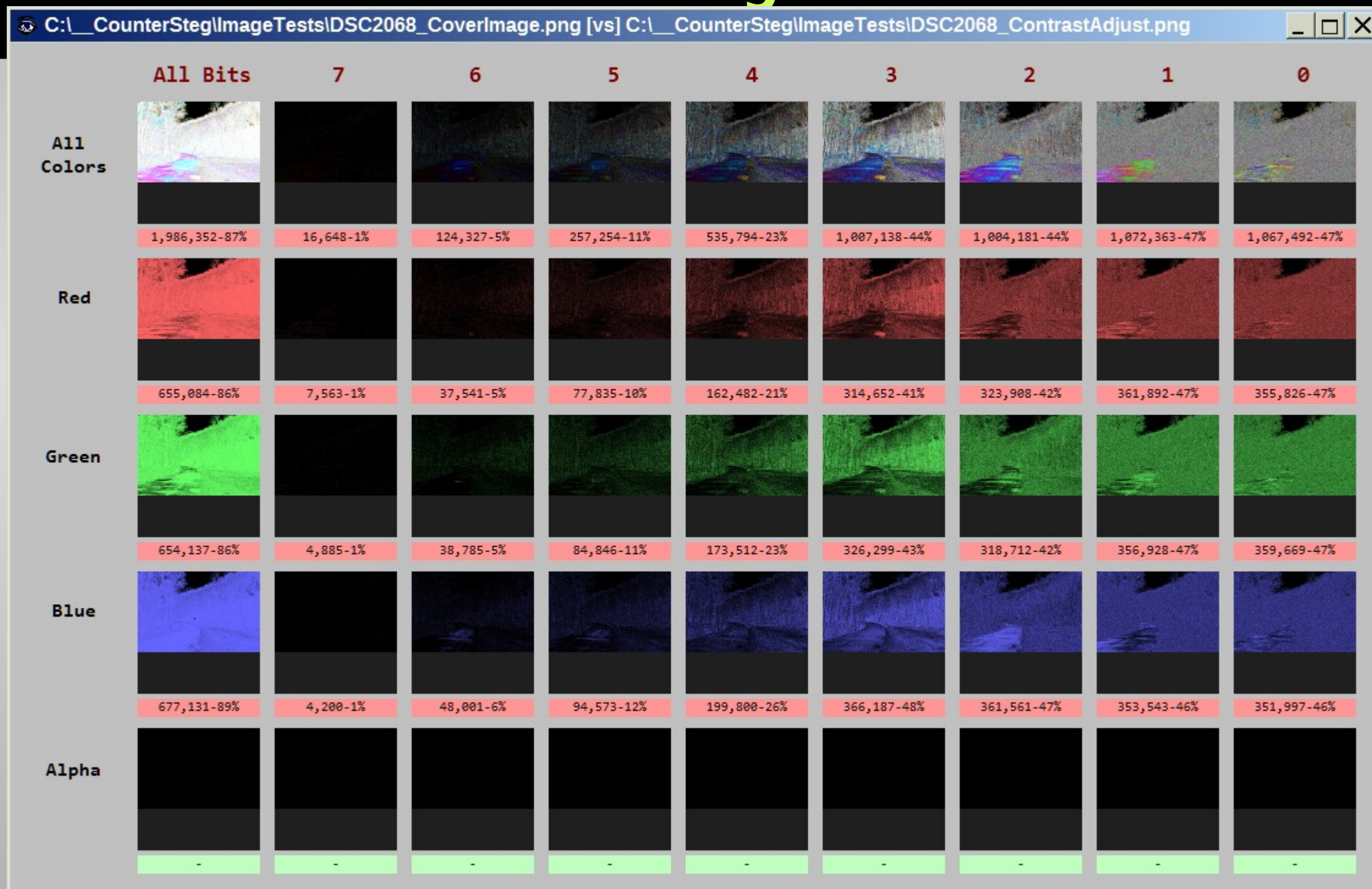


Analysis of cover image

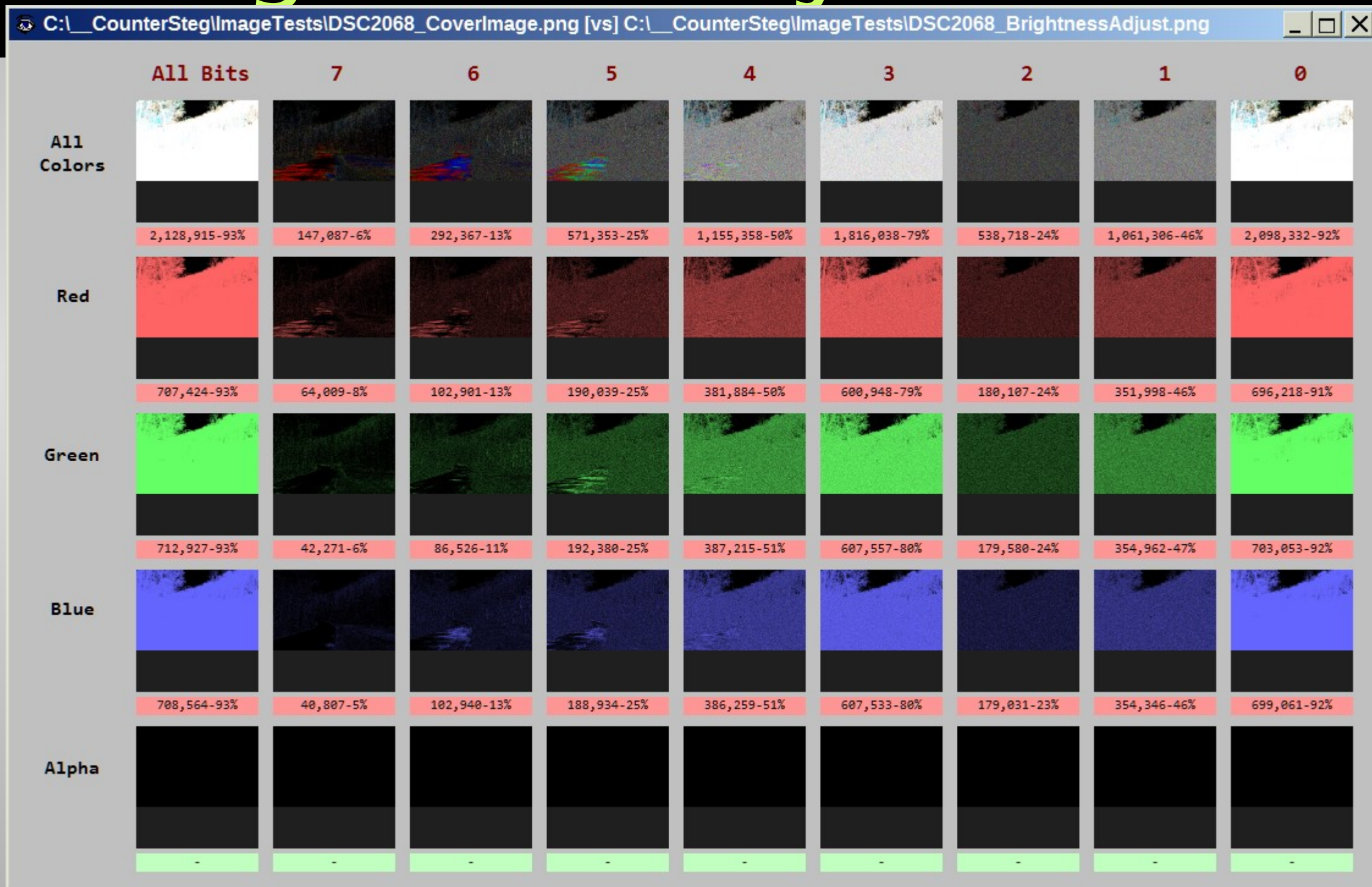




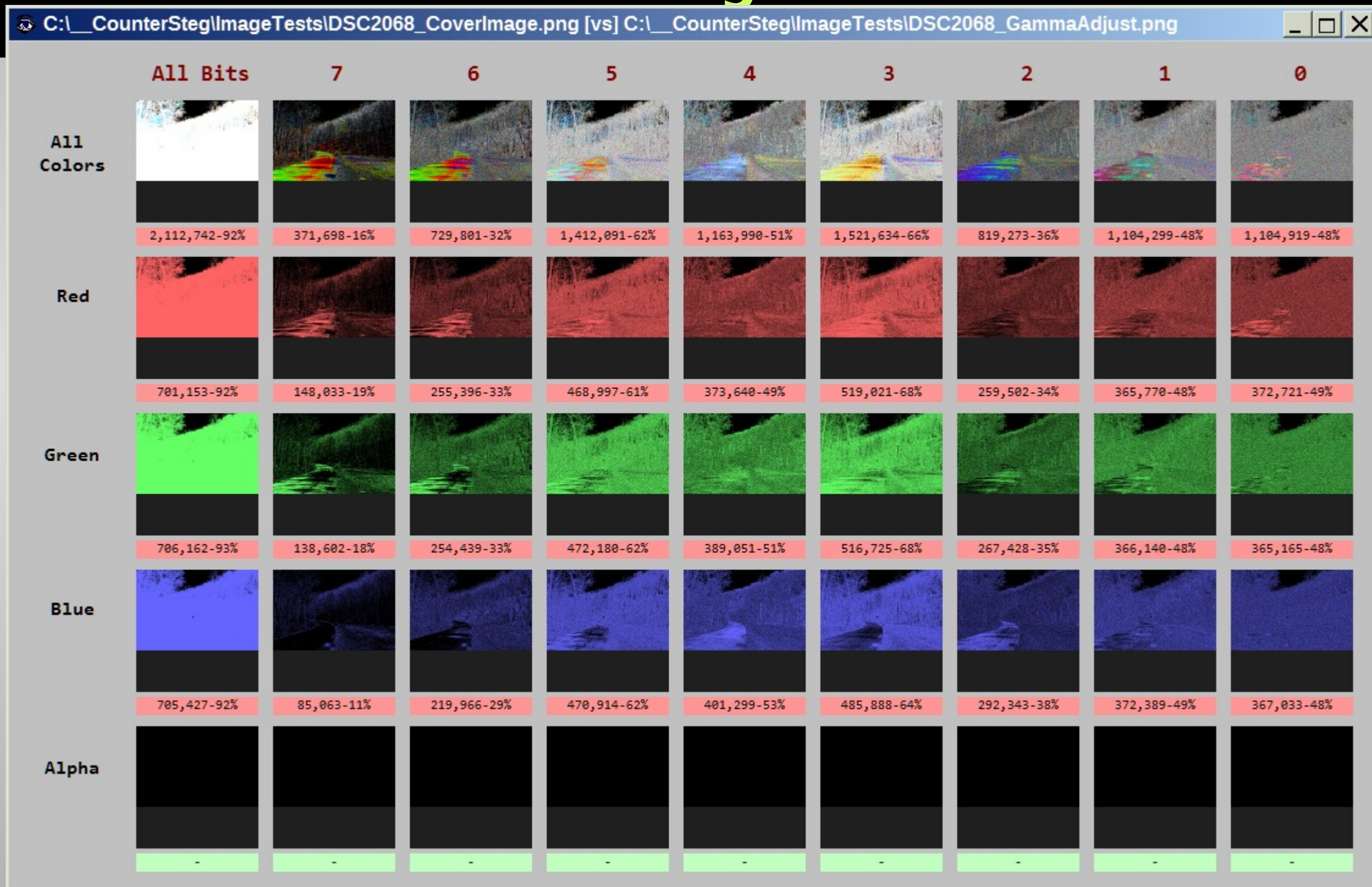
Contrast Adjustment



Brightness Adjustment



Gamma Adjustment



The “Low”

- **Steganography Online** – <http://stylesuxx.github.io/steganography/>
- **StegoShare** – <http://stegosshare.sourceforge.net/>
- **Geocaching Toolbox** – <https://www.geocachingtoolbox.com/index.php?page=steganography>
- **DevFarmSteganography** – <https://devfarm.it/steganography/>

Steganography Online

stylesuxx.github.io/steganography/



Steganography Online

Encode

Decode

Encode message

To encode a message into an image, choose the image you want to use, enter your text and hit the **Encode** button.

Save the last image, it will contain your hidden message.

Remember, the more text you want to hide, the larger the image has to be. In case you chose an image that is too small to hold your message you will be informed.

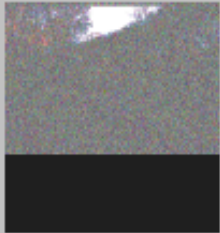




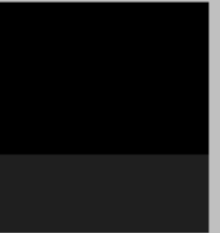


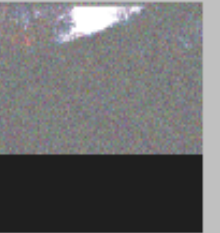
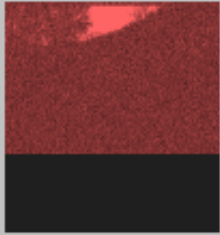




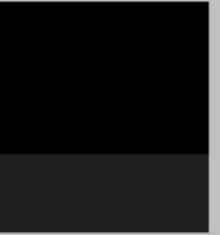
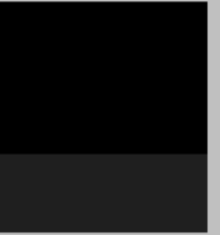


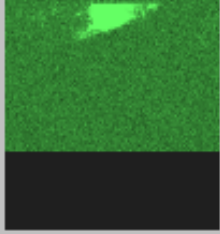



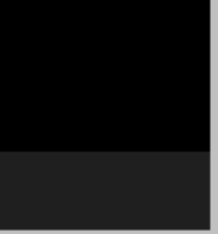
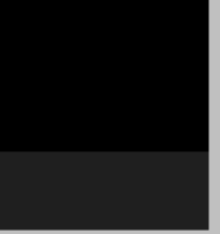
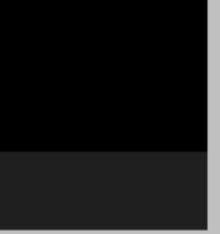
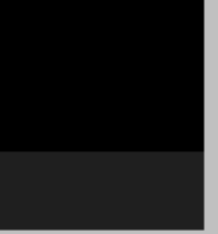
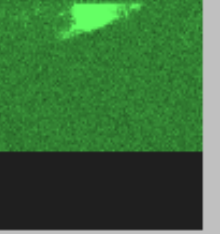
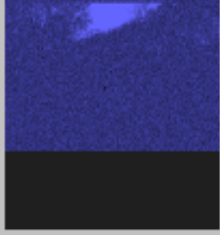




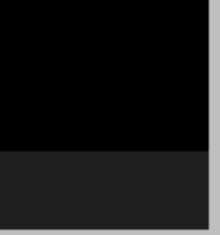

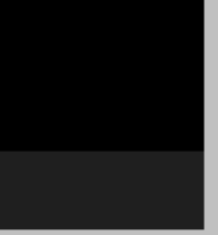
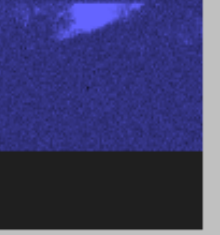









Neither the image nor the message you hide will be at any moment transmitted over the web, all the magic happens within your browser.

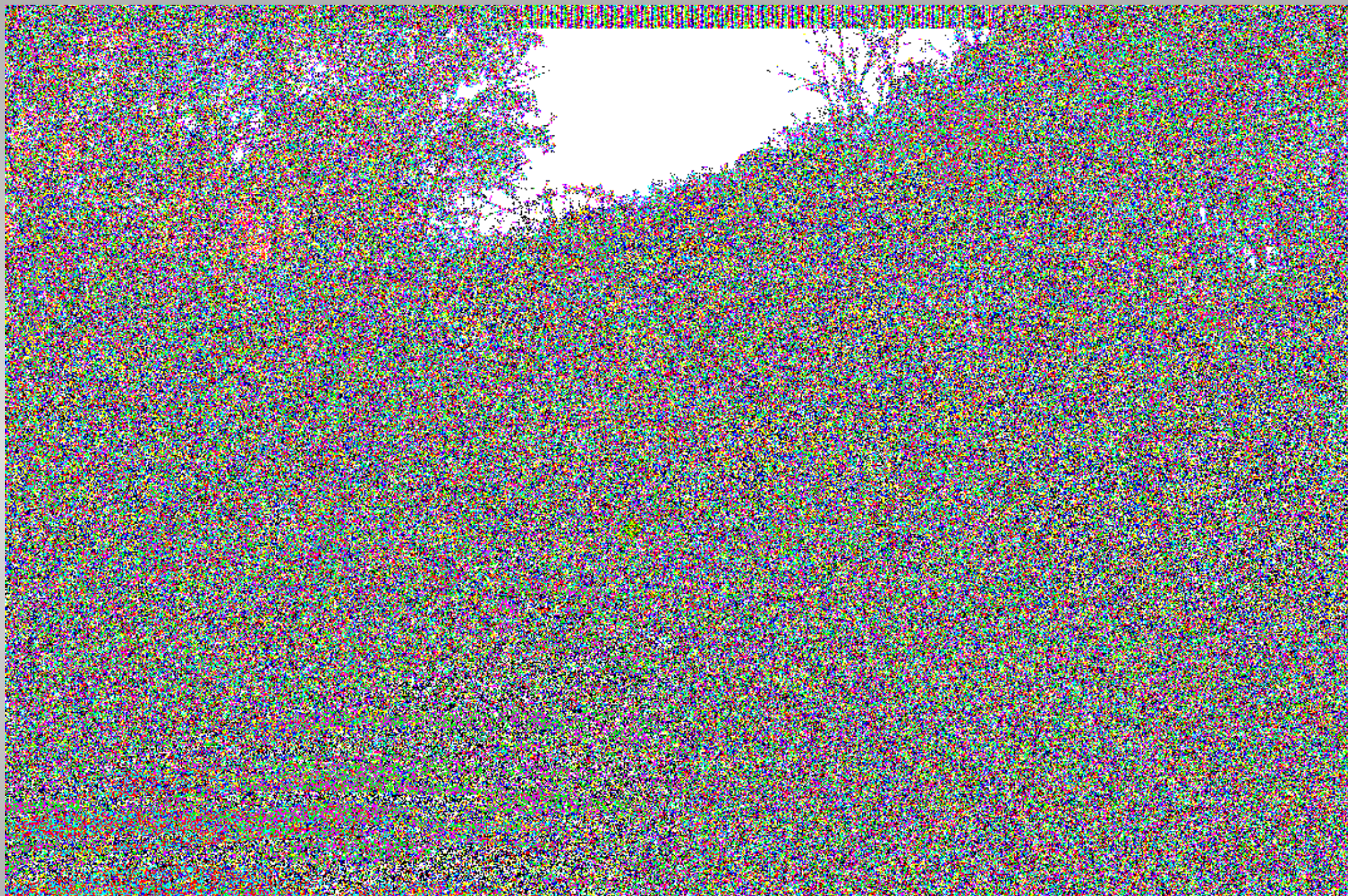
Browse... No file selected.

Enter your message here

Encode

	All Bits	7	6	5	4	3	2	1	0
All Colors									
Red									
Green									
Blue									
Alpha									

	All Bits	7	6	5	4	3	2	1	0
All Colors	 1,210,008-53%	 -	 -	 -	 -	 -	 -	 -	 1,210,008-53%
Red	 403,621-53%	 -	 -	 -	 -	 -	 -	 -	 403,621-53%
Green	 401,396-53%	 -	 -	 -	 -	 -	 -	 -	 401,396-53%
Blue	 404,991-53%	 -	 -	 -	 -	 -	 -	 -	 404,991-53%
Alpha	 763,264-100%	 763,264-100%	 763,264-100%	 763,264-100%	 763,264-100%	 763,264-100%	 763,264-100%	 763,264-100%	 763,264-100%



StegoShare

stegoshare.sourceforge.net



[how it works](#) [screenshots](#) [download](#) [legal help and advices](#) [forum](#)



StegoShare

New anonymous file sharing technology

Want to share censored materials in the Internet without fear of legal prosecution? It is easy now...

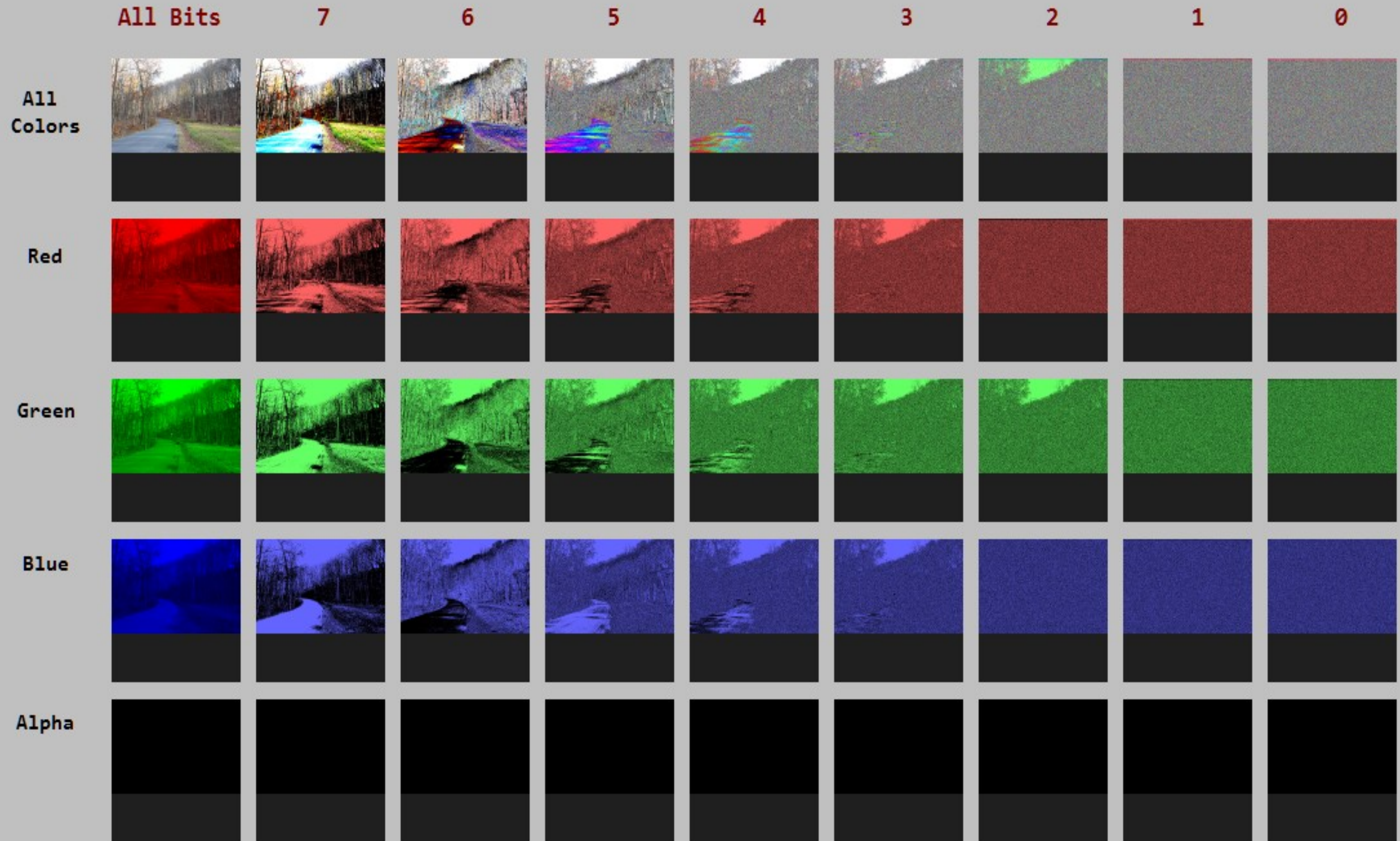
Just 3 steps:

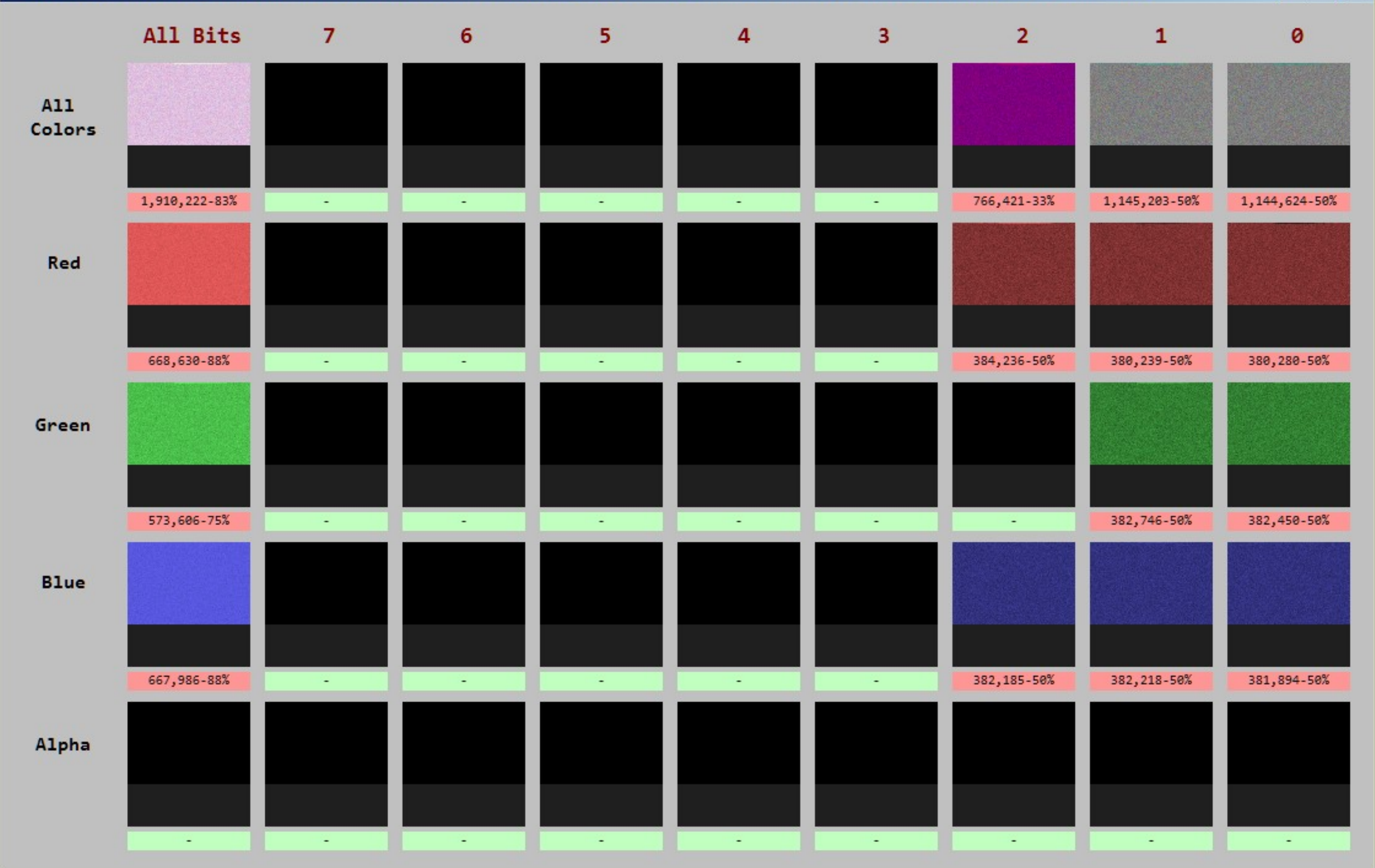
- I. Download legal images from public photo hosting or take photos with your digital camera.
- II. Use StegoShare to embed censored file (which distribution may be illegal in your county) into images, then upload stego images to the photo torrent tracker (or other p2p network) as ordinary legal photos (**human eye cannot detect the difference between original image and picture with included hidden file**). Also post hidden file's description and link to stego images on the private blog/forum (not photo tracker). Read details at the section "[How it works](#)".
- III. Seed (distribute) images with censored file without any fear of legal prosecution or litigation. If you will be caught, **you can always say that you even didn't knew about illicit file, embedded into images** (it is impossible to prove opposite, you have 100% plausible deniability). This protection model can be used as for end users (downloaders and seeders), as also for public photo trackers. Detailed information at the section "[Legal help and advices](#)".

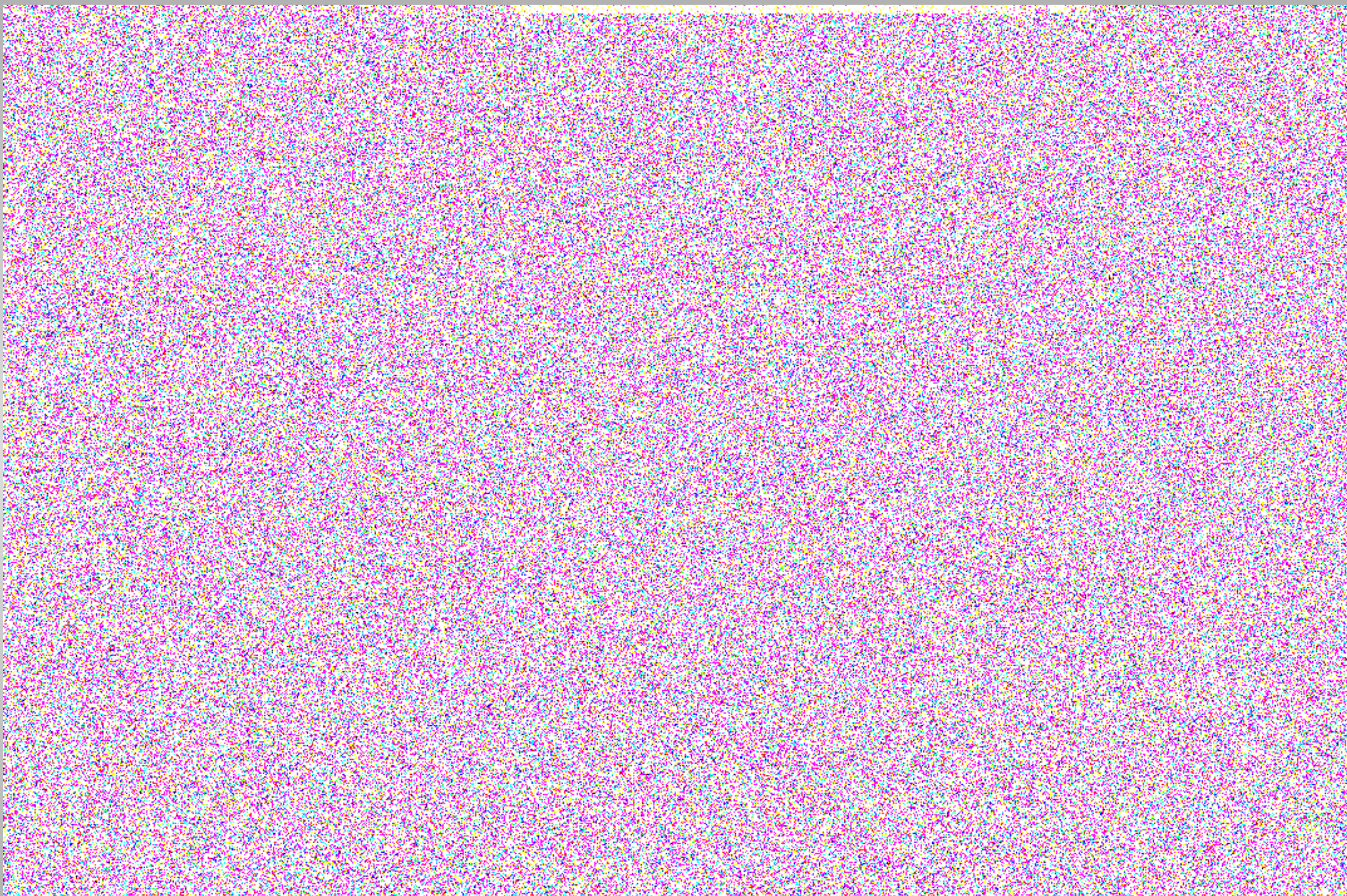


Are interested in?

[Download](#) it now! Try this real [example](#) (11Mb, password "123"). If you have a question, ask on our [forum](#).







Geocaching Toolbox

https://www.geocachingtoolbox.com/index.php?page=steganography



[Geocaching Toolbox](#) ▾ [Geocaching](#) ▾ [FAQ](#) ▾ [Downloads](#) [Links](#) 🇬🇧 [English](#) ▾

Steganography

[Tweet](#)
[Follow](#)
[Share](#)

This tool can be used to hide images and text in an image or to retrieve information from an image. Upload an image or provide the web location of an image and click submit to retrieve the information from it. Did you want to hide information in the image? Continue to upload the secret image or provide the text. Add an optional key to encrypt your data even better and click submit to hide it in the image. Steganography can be applied in many different ways. There can be information in an image while this tool is not able to find anything. Also, other tools might not be able to extract information from encrypted images created by this tool.

Upload image: No file selected.

OR

Location (URL) of the image:

Click submit now to retrieve the message from the image
Continue below to hide a secret in the image.

Encryption key: Optional for additional encryption

Upload secret file: No file selected.

OR

Secret message:

Background

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphei meaning "writing". Since the rise of more and more digital files for image and sound, the interest in steganography is increased.

All Bits

7

6

5

4

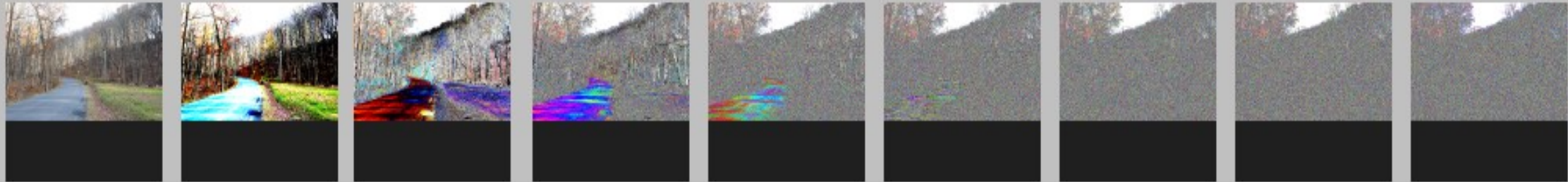
3

2

1

0

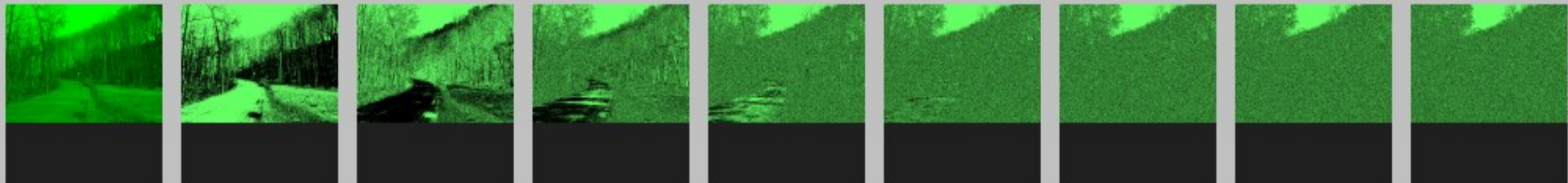
All Colors



Red



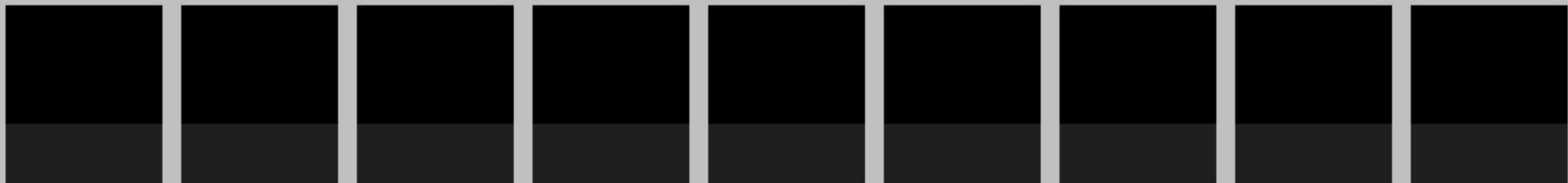
Green



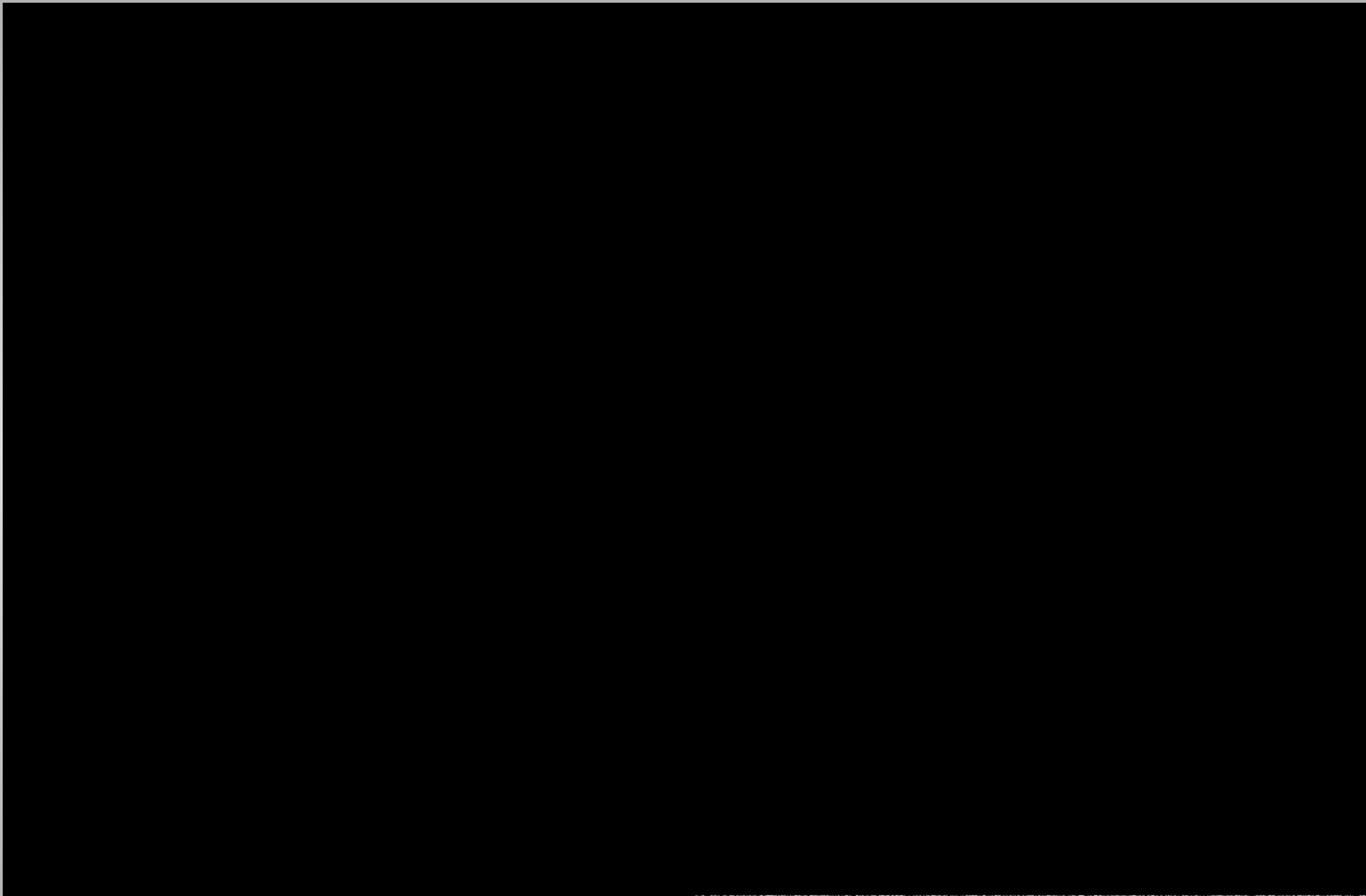
Blue



Alpha



	All Bits	7	6	5	4	3	2	1	0
All Colors									
	18,489-1%	-	-	-	-	-	-	-	18,489-1%
Red									
	6,149-1%	-	-	-	-	-	-	-	6,149-1%
Green									
	6,155-1%	-	-	-	-	-	-	-	6,155-1%
Blue									
	6,185-1%	-	-	-	-	-	-	-	6,185-1%
Alpha									
	-	-	-	-	-	-	-	-	-



Dev Farm Steganography

https://devfarm.it/steganography/

{ DEV FARM } *Web & Windows Development* [FORUM](#) [DOWNLOADS](#) [ONLINE TOOLS](#)

Steganography

This application will hide data inside an image or extract hidden data from an image, you can either supply the image we are encoding/decoding as a URL or upload an image file.

Upload an image file: No file selected. **OR** Supply a URL to the image:

We will encrypt the data before it puts it into the image, this is to insure nobody but the indended parties can extract hidden data from an image, before we can encrypt the data securely we need a key, this is optional.

Please provide a key to encrypt/decrypt data:

Now we need some data to hide in the image you should have provided above, if you are extracting data from an image you can just leave this blank.

Type a secret message to hide in the file:

OR Upload a secret file: No file selected.

All Bits

7

6

5

4

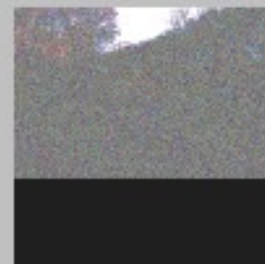
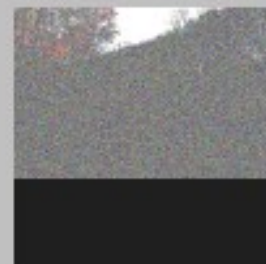
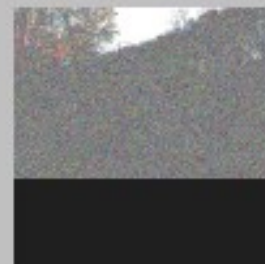
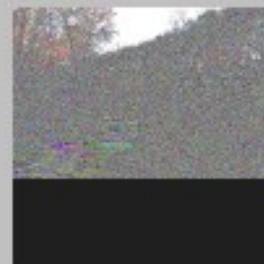
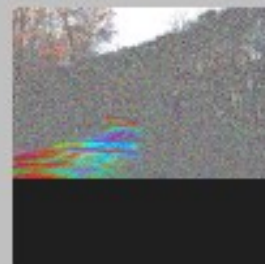
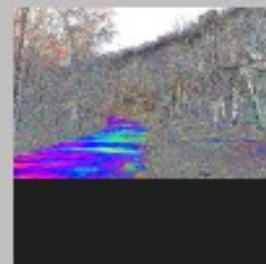
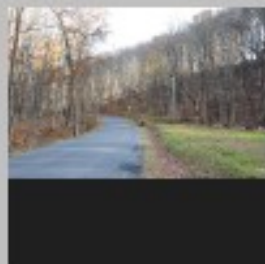
3

2

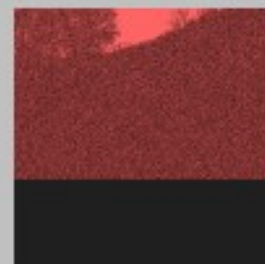
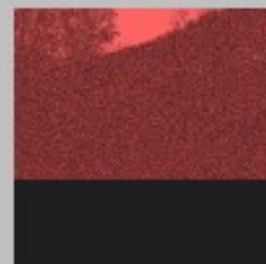
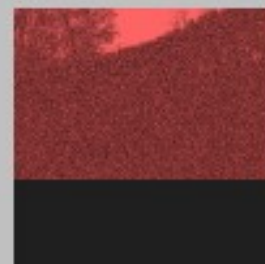
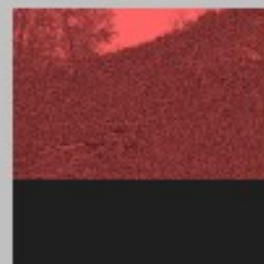
1

0

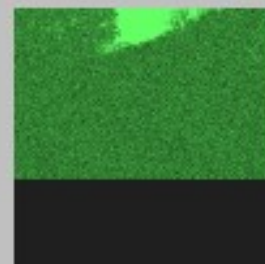
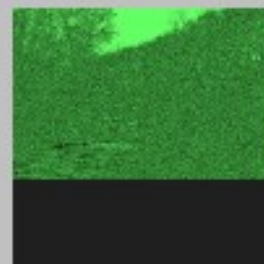
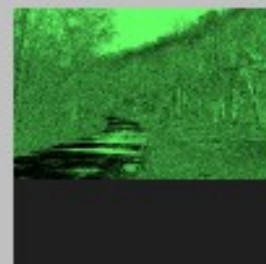
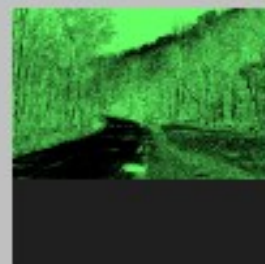
All Colors



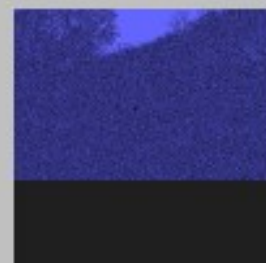
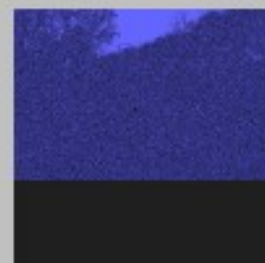
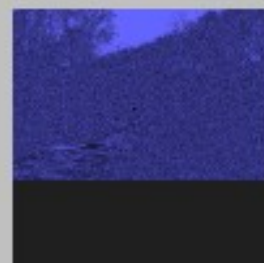
Red



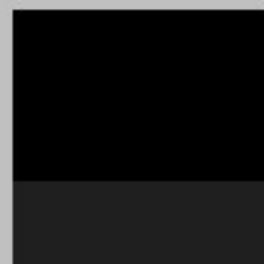
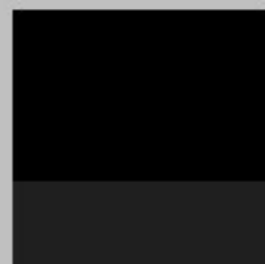
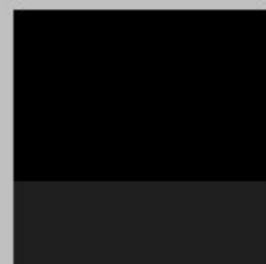
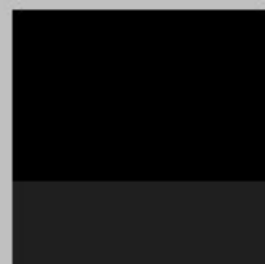
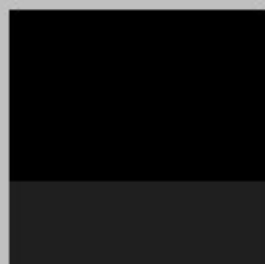
Green



Blue



Alpha



	All Bits	7	6	5	4	3	2	1	0
All Colors									
	18,491-1%	-	-	-	-	-	-	-	18,491-1%
Red									
	6,127-1%	-	-	-	-	-	-	-	6,127-1%
Green									
	6,164-1%	-	-	-	-	-	-	-	6,164-1%
Blue									
	6,200-1%	-	-	-	-	-	-	-	6,200-1%
Alpha									
	-	-	-	-	-	-	-	-	-



The “Mid”

- **f5stego.js** – <http://desudesutalk.github.io/f5stegojs/>
- **BitCrypt** – <http://bitcrypt.moshe-szweizer.com/>
- **OpenPuff** – http://embeddedsw.net/OpenPuff_Steganography_Home.html

f5stego.js

desudesutalk.github.io/f5stegojs/

f5stego.js

JPEG steganography for browser and node.
F5 algo in pure javascript.

[View project on GitHub](#)

// Online demo

Password:

Cover image: No file selected.

Data to embedd: No file selected.

// Overview

This library implements jpeg codec capable of reading Huffman-coded baseline and progressive jpeg files and writing Huffman-coded baseline files. Decompression is done only up to raw DCT coefficients. They are not dequantized or dezigzagged. This coefficients are then used for embedding hidden messages with f5 algorithm.

I decided to make this library because for my projects I need small (this lib is 15kb minified and 5.5kb if gzipped) and fast code what is easy to maintain (and review). Speed mostly considered for extraction process as often I need to process many images at once.

is maintained by [desudesutalk](#).

This page was generated by [GitHub Pages](#) using the Architect theme by [Jason Long](#).

All Bits

7

6

5

4

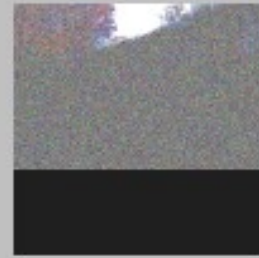
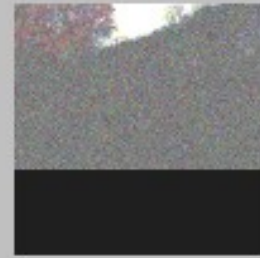
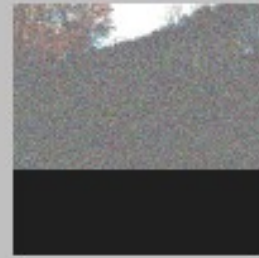
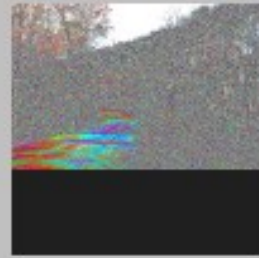
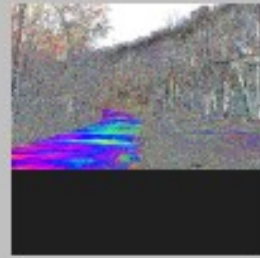
3

2

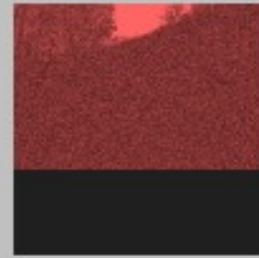
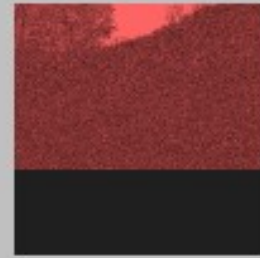
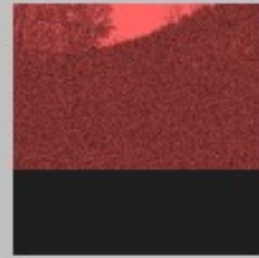
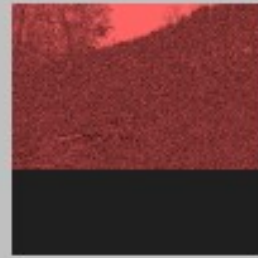
1

0

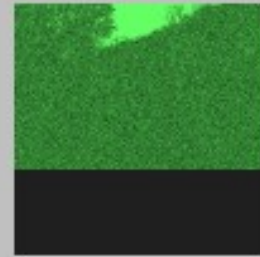
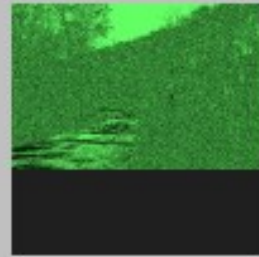
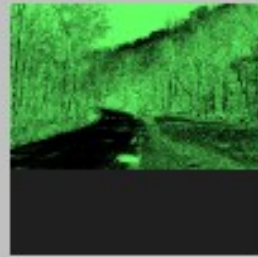
All Colors



Red



Green










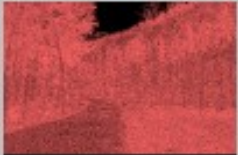






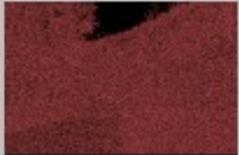

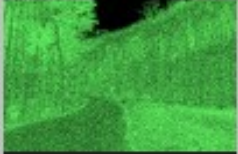






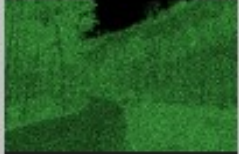

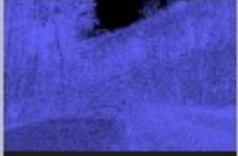




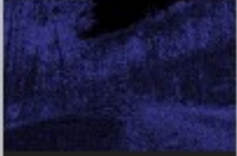
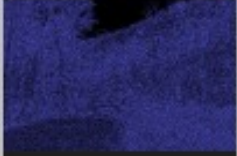

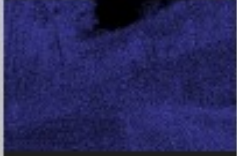











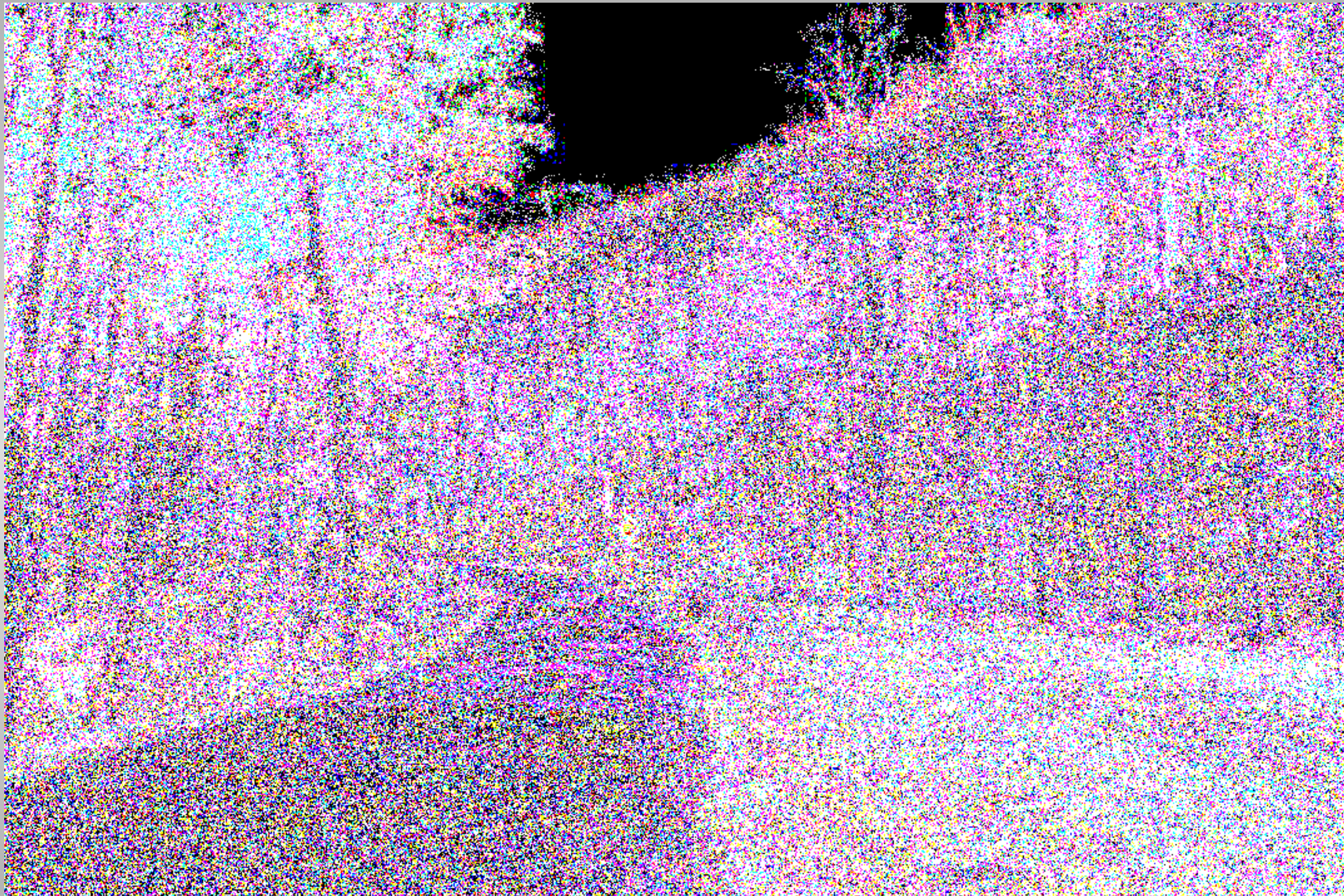
Blue



Alpha



	All Bits	7	6	5	4	3	2	1	0
All Colors	 1,588,339-69%	 30,723-1%	 62,333-3%	 124,629-5%	 249,041-11%	 457,404-20%	 735,965-32%	 951,979-42%	 971,734-42%
Red	 543,158-71%	 12,377-2%	 21,635-3%	 42,356-6%	 85,599-11%	 161,924-21%	 263,723-35%	 319,033-42%	 336,656-44%
Green	 481,721-63%	 5,155-1%	 10,491-1%	 22,162-3%	 46,199-6%	 93,087-12%	 176,895-23%	 287,520-38%	 352,522-46%
Blue	 563,460-74%	 13,191-2%	 30,207-4%	 60,111-8%	 117,243-15%	 202,393-27%	 295,347-39%	 345,426-45%	 282,556-37%
Alpha	 -	 -	 -	 -	 -	 -	 -	 -	 -



BitCrypt

bitcrypt.moshe-szweizer.com



[Welcome](#)
[FAQ](#)
[Purpose](#)
[Technical](#)
[Contact](#)
[Links](#)
[About Author](#)

[Download BitCrypt](#)



BitCrypt

An Ultra-Strong Encryption that is easy to use

So far, no one was able to break into this encryption
but some have tried to discredit it

Moshe Szweizer

A version of BitCrypt called The Privacy Tool, which has a more conventional user interface, may be downloaded from this site [The Privacy Tool](#)

BitCrypt is an elegant encryption utility that allows for storage and transmission of information in an undetectable manner. The software may be used to store plain text and hide it from any third party, or to send information through the means provided by the Internet.

The encryption method consists of two steps in which a user supplied text is concealed within a bitmap image:

- firstly encrypting the text with the ciphers,
- subsequently storing the encrypted text within a user selected bitmap image.

This later step is called steganography, which means "to hide in an invisible manner".

The software hides from the user the complexity of its inner workings. In fact BitCrypt is designed to be easy to use, and requires only a few steps to perform the task of storing and retrieving the text.

The strength of both the initial encryption together with the subsequent steganographic implementation makes the encryption not possible to be broken into. This is to the extend of contemporary supercomputer techniques not being capable of breaking the encryption. The only weak point being the key supplied by the user.

BitCrypt is a boutique style programme designed for those who require the strongest encryption possible. It is provided with a request of being used for legal purposes only.

All Bits

7

6

5

4

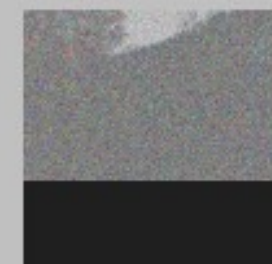
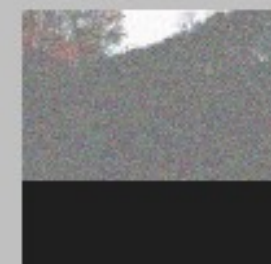
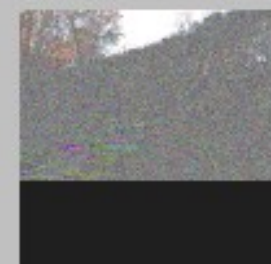
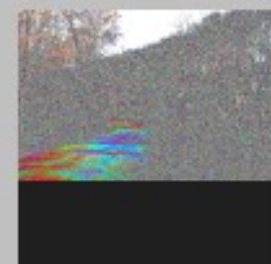
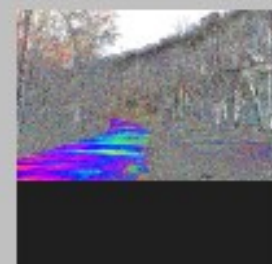
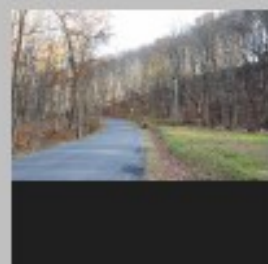
3

2

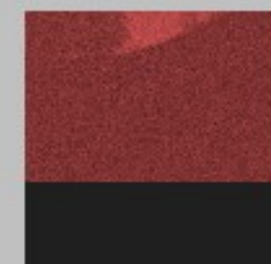
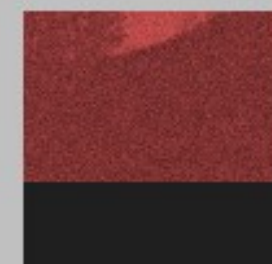
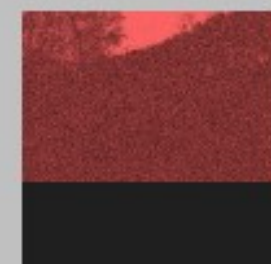
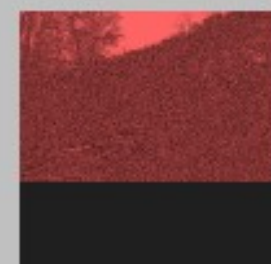
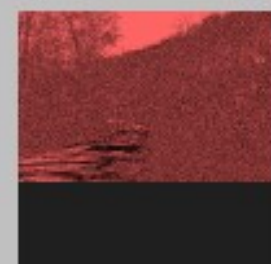
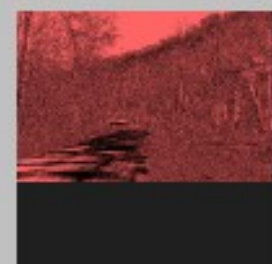
1

0

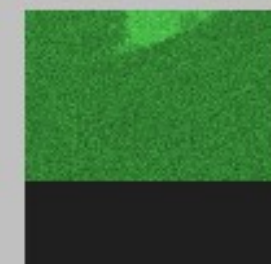
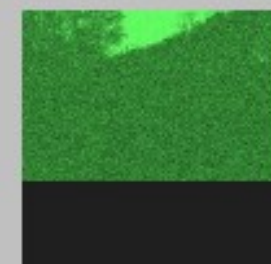
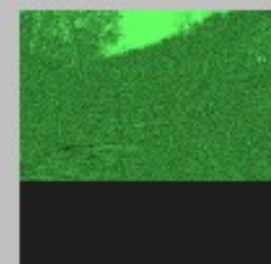
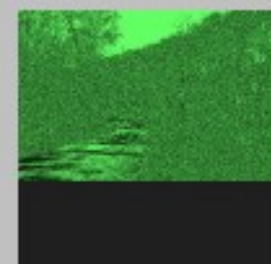
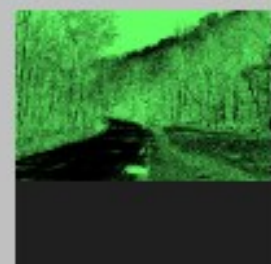
All Colors



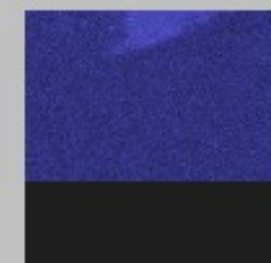
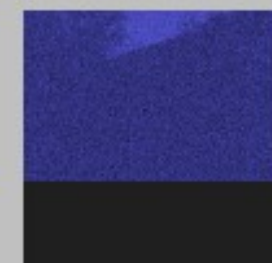
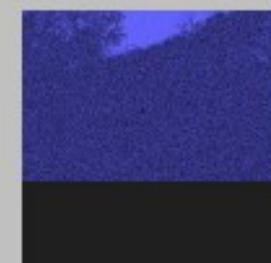
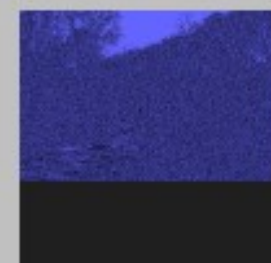
Red



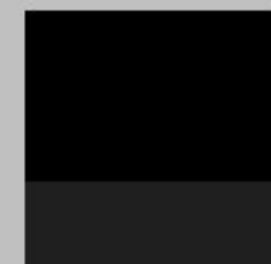
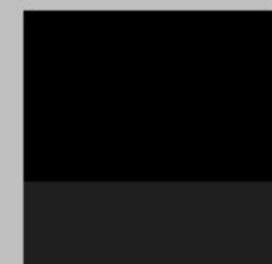
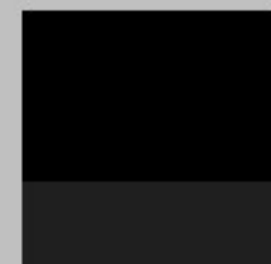
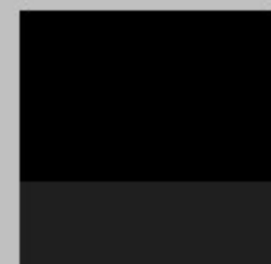
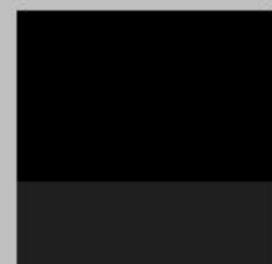
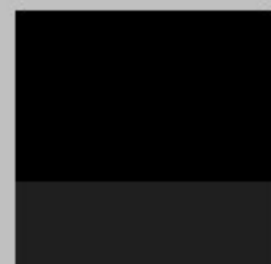
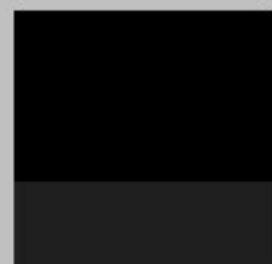
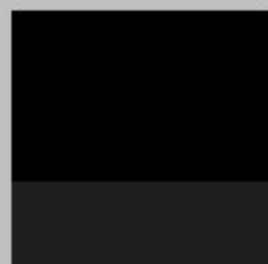
Green

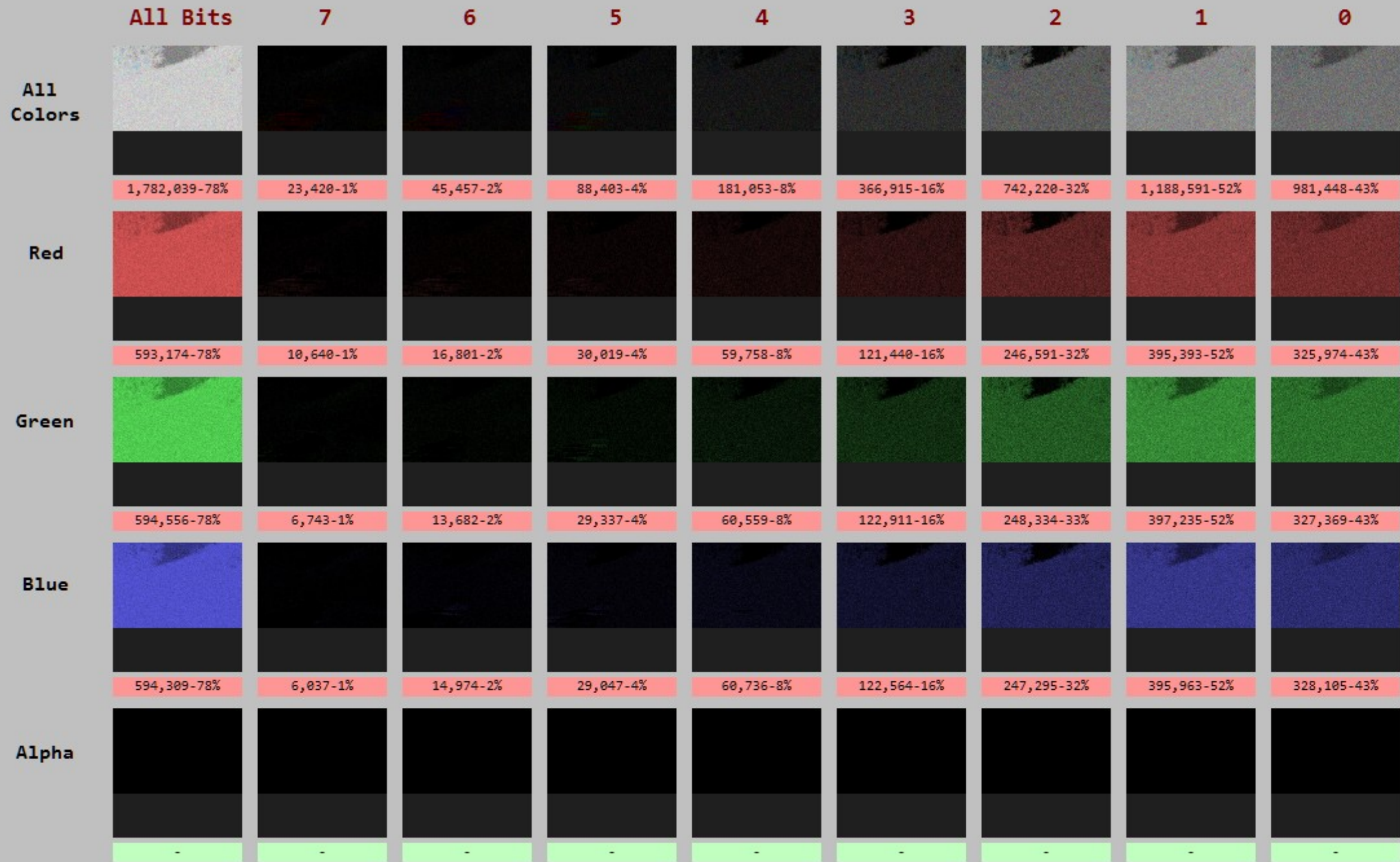


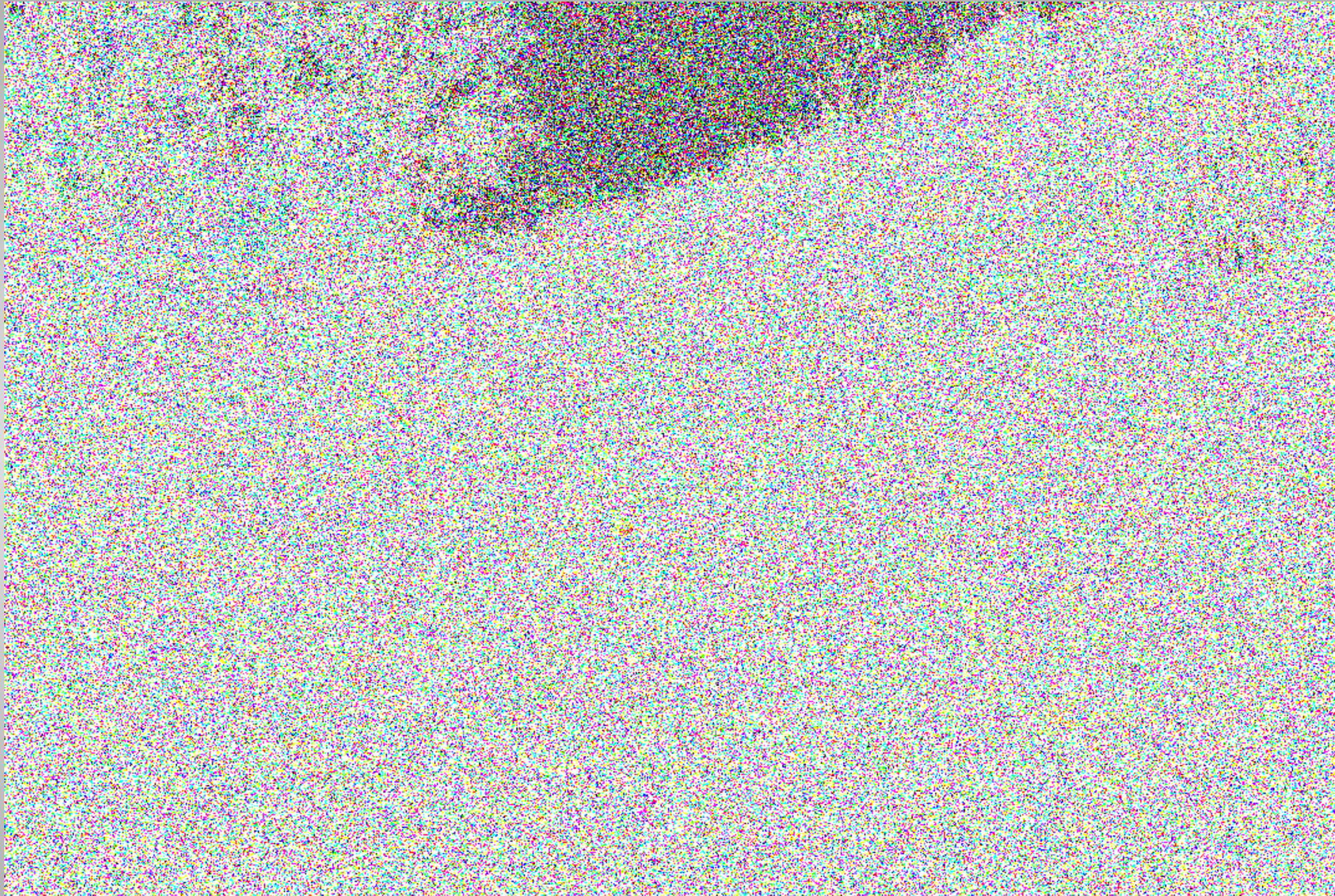
Blue



Alpha







OpenPuff

https://embeddedsww.net/OpenPuff_Steganography_Home.html

INFO@EMBEDEDSW.NET

Facebook YouTube Twitter +1 949-287-8623 SKYPE


Home About Us Security & Software Hardware & Machinery Resources

EMBEDED SW

Delivering Advanced & Reliable Innovation

HOME > SOFTWARE > OPENPUFF STEGANOGRAPHY

OpenPuff - Yet *not* another steganography SW



[Download binary for Windows/Linux](#) / [Source Page](#) / [Randomness Test](#)

[Video Tutorials & Youtube](#) / [For Experts](#) / [Papers & Articles](#)

[Thesis](#) / [Lectures](#) / [Web Reviews](#) / [Reference Images for Testing](#)

OpenPuff is a **professional** steganography tool:

- HW seeded random number generator (CSPRNG)
- Deniable steganography
- Carrier chains (up to 256Mb of hidden data)
- Carrier bits selection level
- Modern multi-cryptography (16 algorithms)
- Multi-layered data obfuscation (3 passwords)
- X-squared steganalysis resistance

OpenPuff supports many **carrier formats**:

- Images (BMP, JPG, PCX, PNG, TGA)
- Audio support (AIFF, MP3, NEXT/SUN, WAV)
- Video support (3GP, MP4, MPG, VOB)
- Flash-Adobe support (FLV, SWF, PDF)

OpenPuff is a **portable/stealth** software:

- Native portable structure (no installation, registry keys, .ini files)
- Runs in user mode with DEP on
- Multithread support (up to 32 CPUs) = Faster processing

OpenPuff is **safe**:

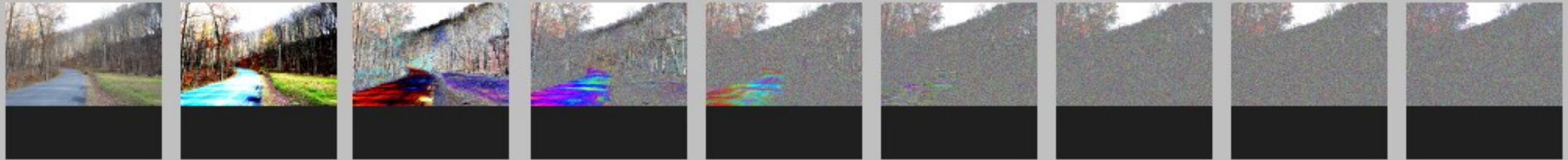
- Spyware/adware-free
- Fully redistributable
- OpenSource core crypto-library (libObfuscate)

Unique layers of **security and obfuscation**:

- 256bit+256bit symmetric-key cryptography (with KDF4 password extension)
- 256bit symmetric-key data scrambling (CSPRNG-based shuffling)
- 256bit symmetric-key data whitening (CSPRNG-based noise mixing)
- Adaptive non-linear carrier bit encoding

All Bits 7 6 5 4 3 2 1 0

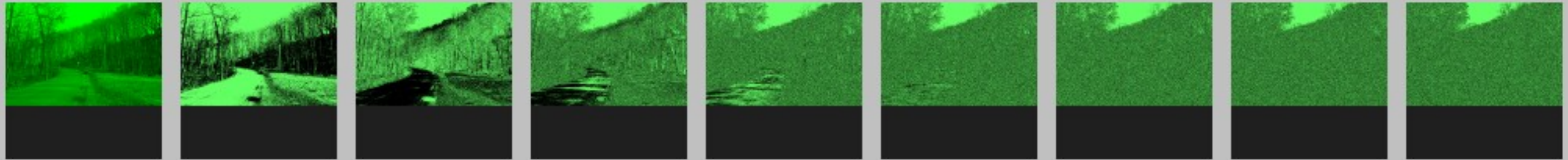
All Colors



Red



Green









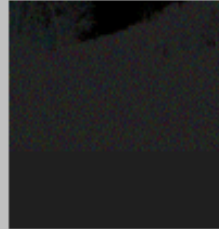








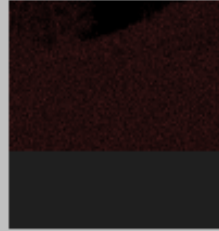
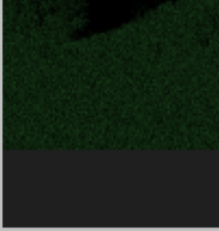








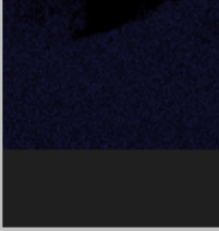



















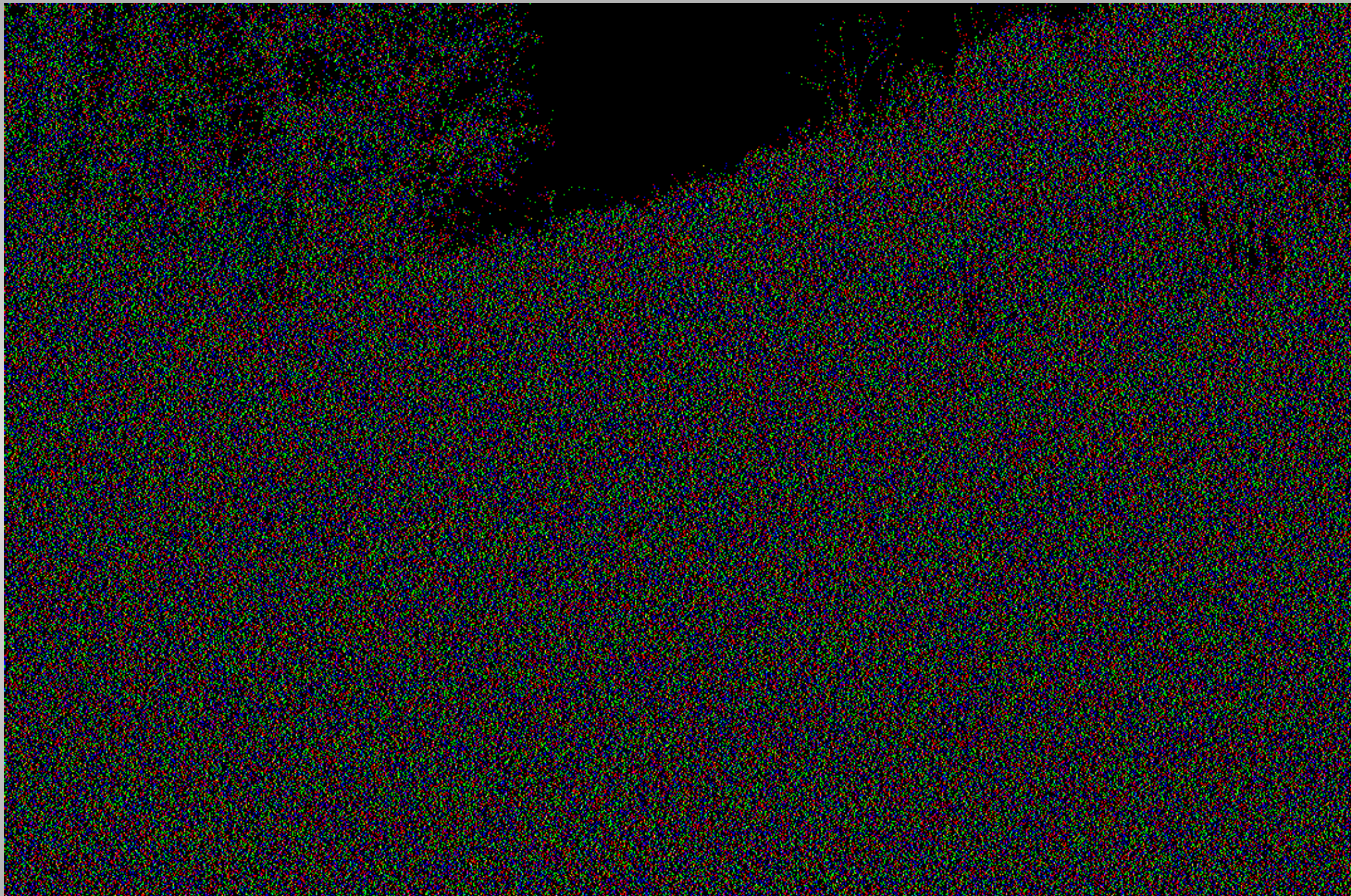
Blue



Alpha



	All Bits	7	6	5	4	3	2	1	0
All Colors	 281,565-12%	 -	 -	 -	 -	 -	 -	 -	 281,565-12%
Red	 93,025-12%	 -	 -	 -	 -	 -	 -	 -	 93,025-12%
Green	 94,277-12%	 -	 -	 -	 -	 -	 -	 -	 94,277-12%
Blue	 94,263-12%	 -	 -	 -	 -	 -	 -	 -	 94,263-12%
Alpha	 -	 -	 -	 -	 -	 -	 -	 -	 -



The “High”

- **OpenStego** –
<https://www.openstego.com/index.html>
- **OTP–Steg** –
<http://www.199.175.52.196.com/OTP–Steg/>

OpenStego

https://www.openstego.com/index.html

OpenStego Home Concepts Features Download About English | Español

Introduction

Welcome to the homepage of OpenStego, the free steganography solution.

OpenStego provides two main functionalities:

- **Data Hiding:** It can hide any data within a cover file (e.g. images).
- **Watermarking (beta):** Watermarking files (e.g. images) with an invisible signature. It can be used to detect unauthorized file copying.

Please see [Concepts](#) page to learn more.

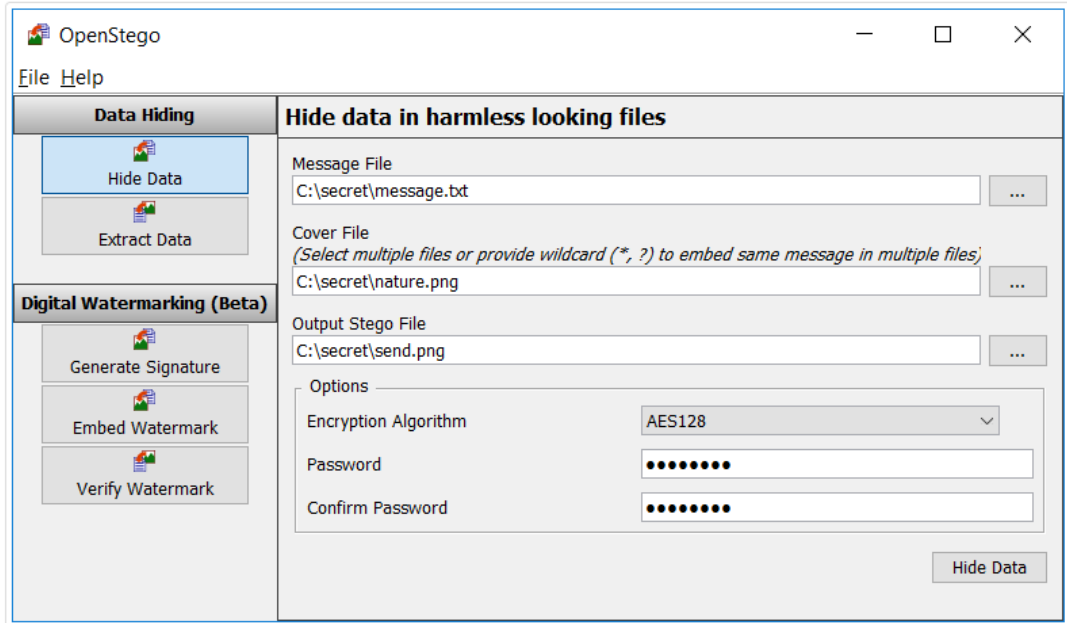
Using OpenStego

Using OpenStego is pretty straightforward. There are two modes of operation - data hiding and watermarking.

Data Hiding

In this mode, you can either hide the data (file) inside an image or extract the data from the image. Check screenshots below to see how it can be done:

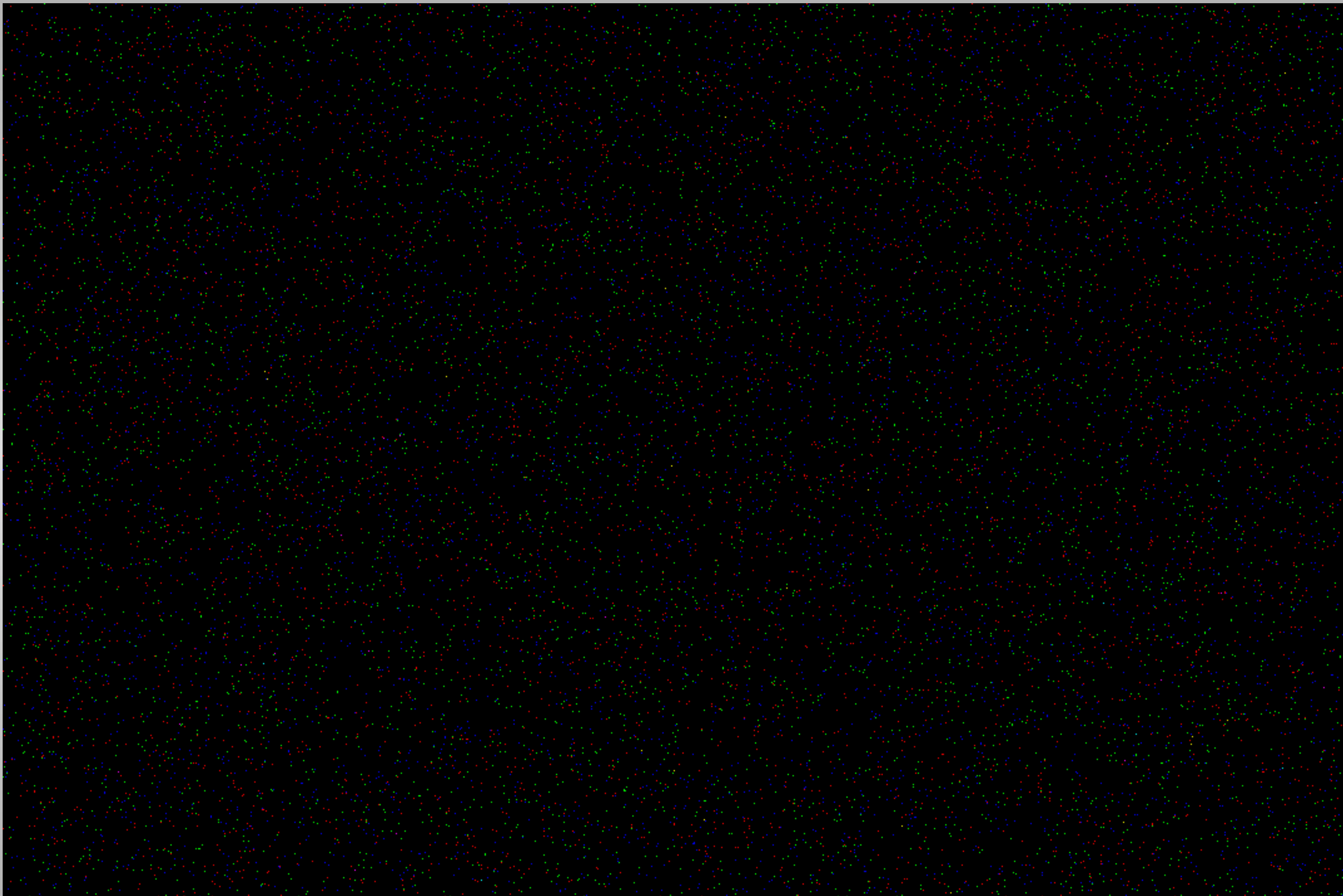
Hide data



The screenshot shows the OpenStego application window. The title bar reads 'OpenStego'. Below the title bar is a menu bar with 'File' and 'Help'. The main interface is divided into two sections: 'Data Hiding' and 'Digital Watermarking (Beta)'. The 'Data Hiding' section is currently selected and contains two buttons: 'Hide Data' and 'Extract Data'. The 'Digital Watermarking (Beta)' section contains three buttons: 'Generate Signature', 'Embed Watermark', and 'Verify Watermark'. The right-hand side of the window is titled 'Hide data in harmless looking files' and contains several input fields and a button. The 'Message File' field contains 'C:\secret\message.txt'. The 'Cover File' field contains 'C:\secret\nature.png' and has a note: '(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)'. The 'Output Stego File' field contains 'C:\secret\send.png'. Below these fields is an 'Options' section with a dropdown menu for 'Encryption Algorithm' set to 'AES128', and two password fields labeled 'Password' and 'Confirm Password', both containing seven dots. A 'Hide Data' button is located at the bottom right of the options section.

	All Bits	7	6	5	4	3	2	1	0
All Colors									
Red									
Green									
Blue									
Alpha									

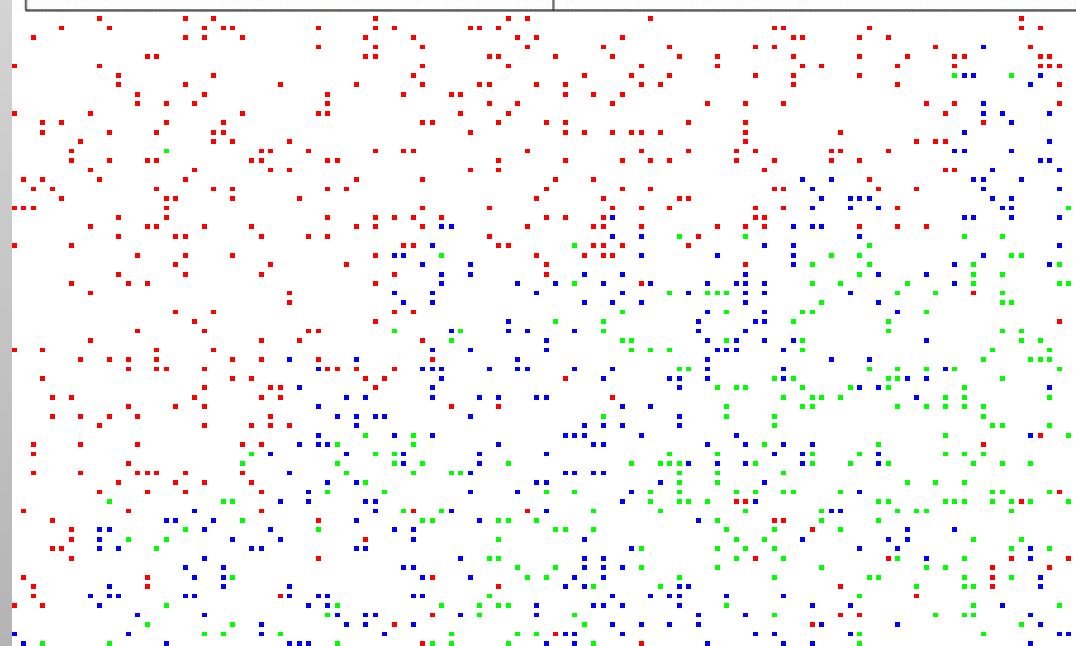
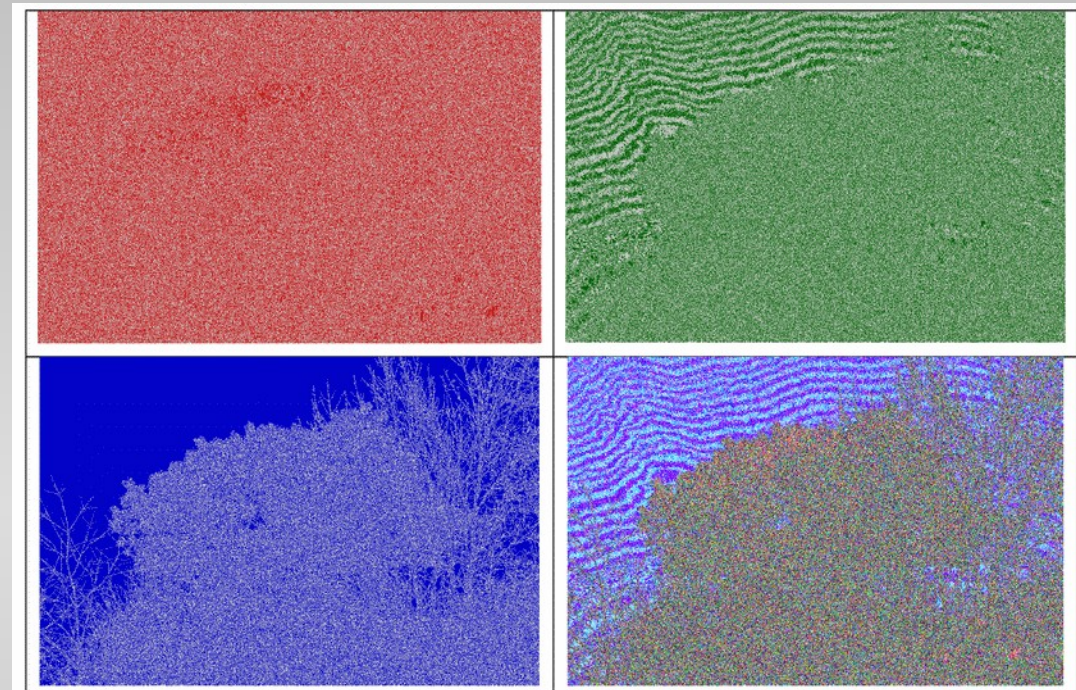
	All Bits	7	6	5	4	3	2	1	0
All Colors									
	14,021-1%	-	-	-	-	-	-	-	14,021-1%
Red									
	4,661-1%	-	-	-	-	-	-	-	4,661-1%
Green									
	4,698-1%	-	-	-	-	-	-	-	4,698-1%
Blue									
	4,662-1%	-	-	-	-	-	-	-	4,662-1%
Alpha									
	-	-	-	-	-	-	-	-	-



OTP-Steg (One-Time-Pad Steg)

<http://199.175.52.196/OTP-Steg/>

The screenshot shows the 'OTP-Steg-[Encrypt]' web application interface. It features a message area with text in multiple languages (English, Russian, Chinese, Japanese, Georgian, Hebrew, Hindi, Vietnamese, Arabic) explaining the One-time pad (OTP) concept. The interface includes a 'Message' field with '3,370B/0.295%' and a toolbar with options like 'F', 'A+', 'A-', 'B', 'P', 'Colors', 'Copy', 'Paste', and 'Clear'. Below the message area, there are sections for 'Select Image:' and 'Select Key:'. The 'Select Image:' list includes files like 'beatgirl_01k.bmp', 'Black01.png', 'boom.bmp', 'boom_01k.bmp', 'boom_02k.bmp', 'bridge.png', 'googlemondrian.bmp', 'googlemondrian_02k.bmp', 'Greece.png', 'GreeceLarge.png', 'NYC01.png', 'NYC02.png', 'NYC03.png', 'Paris.jpg', 'raven.jpg', 'White01.png', and 'X000000_Z010000_Falluj'. The 'Select Key:' field shows '2015-12-03.png'. The interface also displays 'Enc: 99.93% Same: 00.56% Blk: 00.00% Wht: 00.00%' and '97.19% - OK'. At the bottom, there are 'File Type' options (PNG, BMP, Other, JP2), 'File Name Prefix', 'Status' (Encrypted Image Saved. 09166.png [38 Seconds]), 'Key Delimiters' (<n| \$Ã-iH\ç><ÃfN" "%pH2è><11 >), 'LSB Altered: 0.173% / 0.010bpp', and a SHA256 hash: 79110FB42F7D0D4686C6A0A6FEBD7AC3A85A815F0D6EBD46548F57359E25C8F1.



All Bits

7

6

5

4

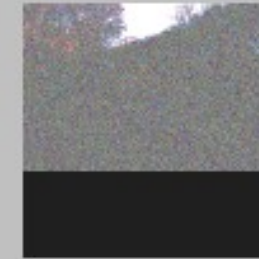
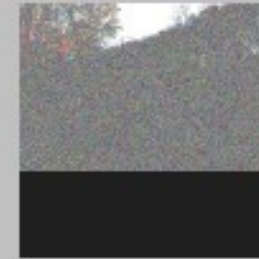
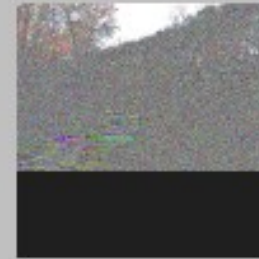
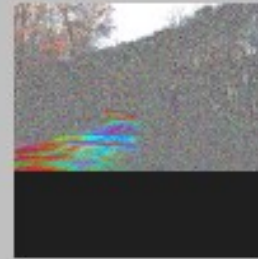
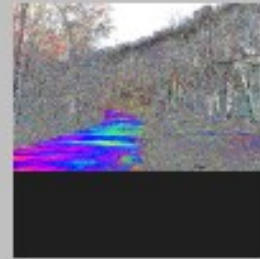
3

2

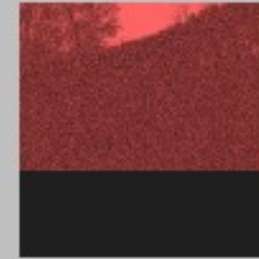
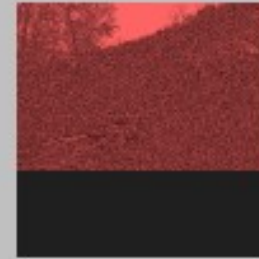
1

0

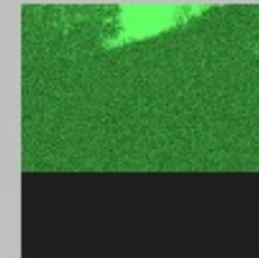
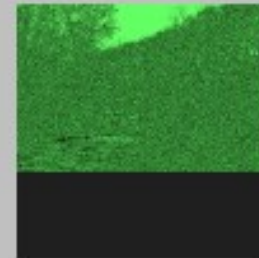
All Colors



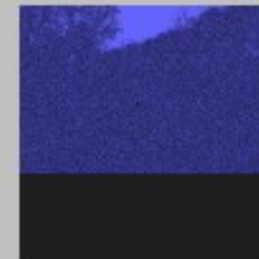
Red



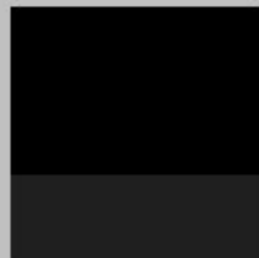
Green

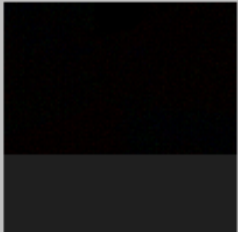







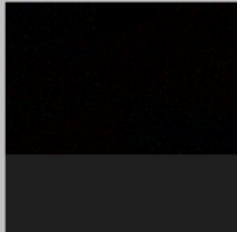
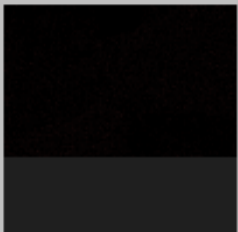







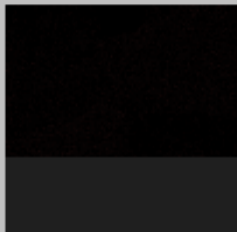
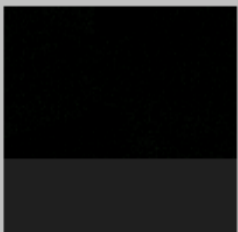







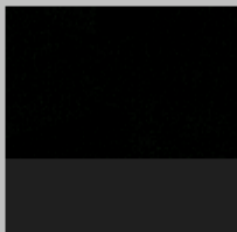
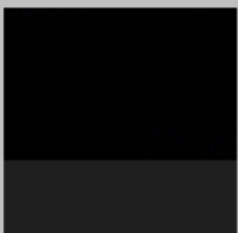
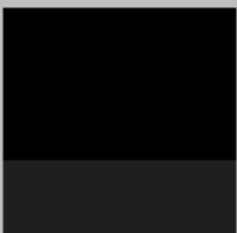
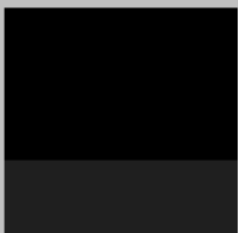
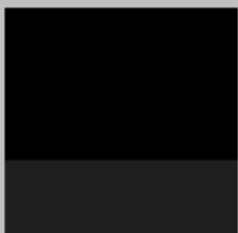
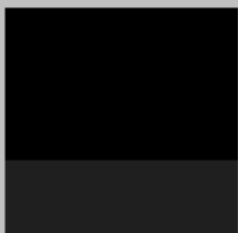
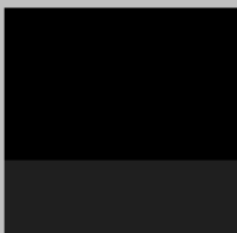
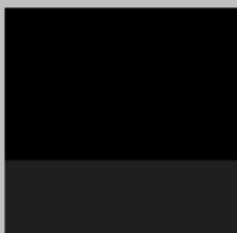
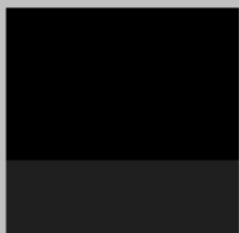
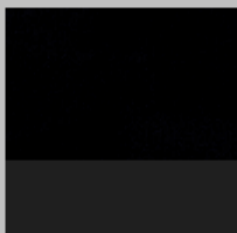
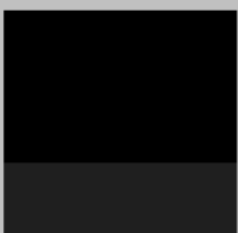
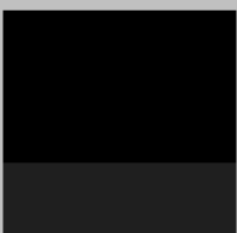
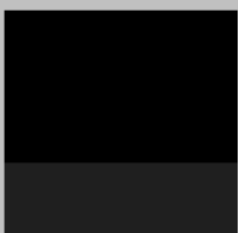
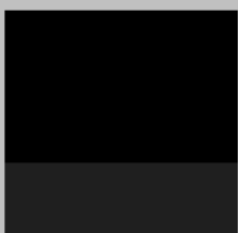
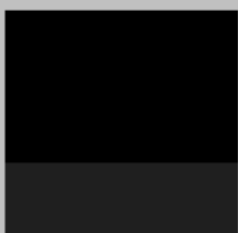
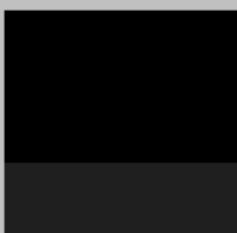
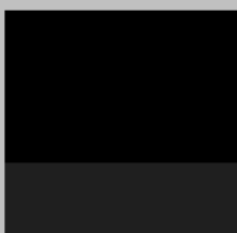
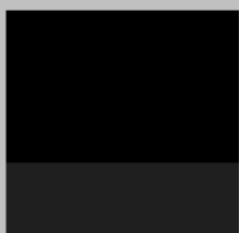
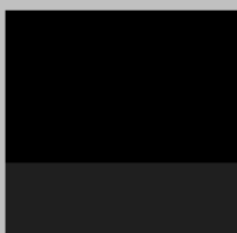


Blue



Alpha



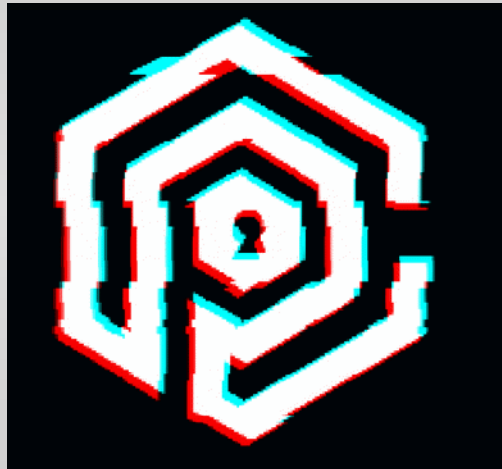
	All Bits	7	6	5	4	3	2	1	0
All Colors	 16,868-1%	 -	 -	 -	 -	 -	 -	 -	 16,868-1%
Red	 9,986-1%	 -	 -	 -	 -	 -	 -	 -	 9,986-1%
Green	 3,564-0%	 -	 -	 -	 -	 -	 -	 -	 3,564-0%
Blue	 3,318-0%	 -	 -	 -	 -	 -	 -	 -	 3,318-0%
Alpha	 -	 -	 -	 -	 -	 -	 -	 -	 -



Conclusion

- Positively detecting the use of steganography in digital image files currently generally results in an unreliable and inconclusive effort.
- Instead of performing statistical analysis to overall produce subjective results, if steganography is suspected, an investigator would be more effective in simply looking for the original image file for comparison.
- If malware is suspected, compare with similar images and examine for steganographic artifacts.

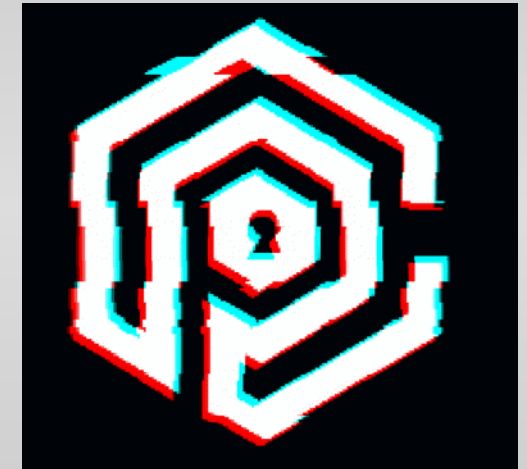
Thank You



Michael Pelosi

mpelosi@tamut.edu

903-334-6744



Texas A&M University, Texarkana, Texas