

Rygelock User Guide



RYGELOCK STEGANOGRAPHY SYSTEM BY SHARVEEN MURTHI

USE FOR SAFEGUARD YOUR SENSITIVE INFORMATION WITH STEGANOGRAPHY. WITH THE SOURCE CODE YOU CAN HAVE YOUR OWN RYGELOCK TO YOUR DESIRE OR USE PART OF RYGELOCK FOR YOUR STEGANOGRAPHY SYSTEM. PLAY AROUND, TEST & TRAIN YOUR DIGITAL FORENSIC SKILLS BREAKING RYGELOCK'S SECURITY AND STEGANOGRAPHY

!!! Rygelock is for academic use only. Do not use it for malicious purposes!!!

Table of Contents

1. Prerequisites	2
2. Install & Launch	2
2.1 Launching the project	2
2.2 Use the Standalone executable	2
3. UI	3
3.1 Main Menu	3
3.2 Hide Panel	4
3.3 Unhide Panel	10
3.4 Rygelock_Output Contents	13
3.5 Settings Panel	14
4. File Support & Tips	15
5. Troubleshooting	15

1. Prerequisites

If Planning to run the project scripts, execute the following commands in terminal:

```
python -m venv .venv
# Windows:
.venv\Scripts\activate

pip install --upgrade pip
pip install -r requirements.txt
```

Or use the existing virtual environment.

2. Install & Launch

2.1 Launching the project

In your IDE run the **rygel.py**. Or execute the command:

```
python rygel.py
```

2.2 Use the Standalone executable

Rygelock has been packaged and build into an executable, **Rygelock.exe**. Just install it and double click the .exe to use Rygelock.

Program Name	Rygelock.exe
Size	105MB
MD5	027b37e23eff71bbb89afdfb8ccca2fe
SHA-1	7b182c654a400e5950d20289840dfe11adf7c5cf
SHA-256	bdd4f7b541dde8445a79e50f3d8ccdeac184fcaa05a8976f5a57bab5eef1df52

Table 1 Rygelock Executable Information

3. UI

3.1 Main Menu

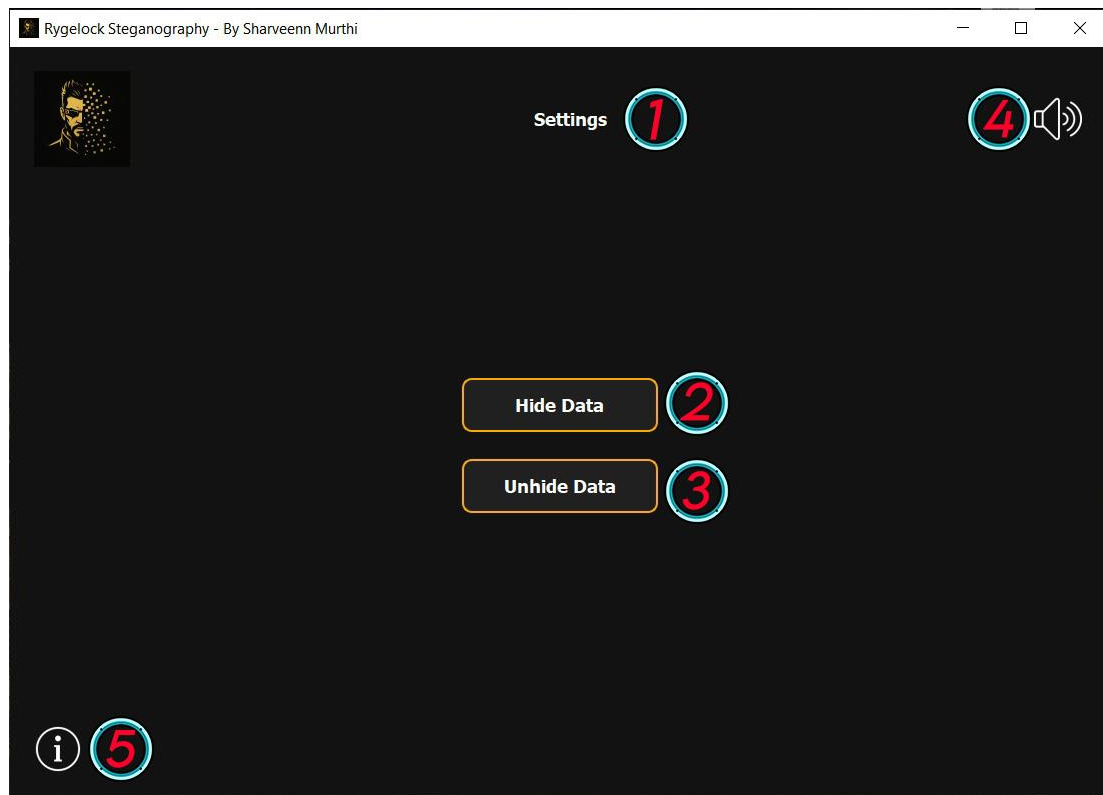


Figure 1 Rygelock Main Menu

1 – Settings

Upon clicking the settings option, user will be redirected to settings panel

2 – Hide Data

Upon clicking the Hide Data option, user will be redirected to Embedding / Hide Panel.

3 – Unhide Data

Upon clicking the Unhide Data option, user will be redirected to extraction/ Hide Panel.

4 – Mute/Unmute Button

Button for both mute and unmute. Users can click the button to disable and enable all system audio.

5 – Information Button

Button for see user technical manual of Rygelock.

3.2 Hide Panel

The screenshot shows the 'Hide Panel' interface for Rygelock Embedding. It features a dark theme with yellow and red accents. At the top left is a 'Back' button (1) and a list of supported file formats: PNG, JPG, jpeg, bmp, tiff, MP4, MP3. At the top right is a 'c' button (2). The main area is divided into four quadrants. The top-left quadrant is for 'Carrier File(s)' with a large empty box. The top-right quadrant is for 'Payload File(s)' with a large empty box. The bottom-left quadrant is for 'Encryption Layers' (3), containing an 'Encryption (Optional)' section with radio buttons for AES (5), Blowfish, and Fernet, a 'Password (Required)' field, a message 'A password is required for AES encryption.', a 'Generate Key' checkbox (6), an 'Enable Masking' checkbox (7), and a 'Layers' dropdown menu set to 'None (1 Layer Total)' (8). The bottom-right quadrant is for 'Deception Mechanism' (4), containing a 'Decoy File' section with a large empty box, an 'Add Decoy Payload' button (9), and a 'Fake password' field. At the bottom center is a 'Start Hiding' button (10).

Figure 2 Rygelock Embedding / Hide Panel

1 – Back Button

Button to get back to main menu.

2 – Reset Button

Button to reset entire Hide Panel

3 – Add Carrier File

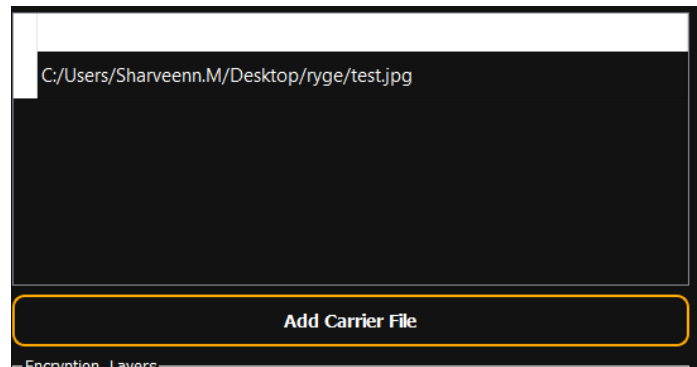


Figure 3 Carrier File Panel

To add carrier files / container for hidden data. Users can click the **Add Carrier File** button to select the carrier file. Users can only choose one carrier file.

Currently Supported Carrier File types:

png, JPG, jpg, jpeg, bmp, tiff, MP4, MP3

Rygelock will be worked further to support more carrier file types in the future.

Rygelock currently uses single carrier file operation. Will be worked further to support multiple carrier files for single operation in the future.

4 – Add Payload File

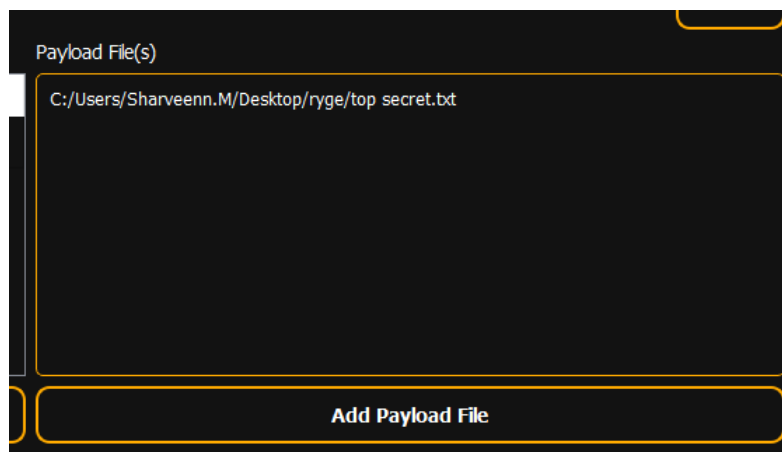


Figure 4 Payload File Panel

To add genuine payload file/ file user wants to hide. Users can click the **Add Payload File** button to select the payload file. Users can only choose one payload file. It can be any type.

Rygelock currently operates single payload file operation. Will be worked further to support multiple payload files for single operation in the future.

5 – Encryption

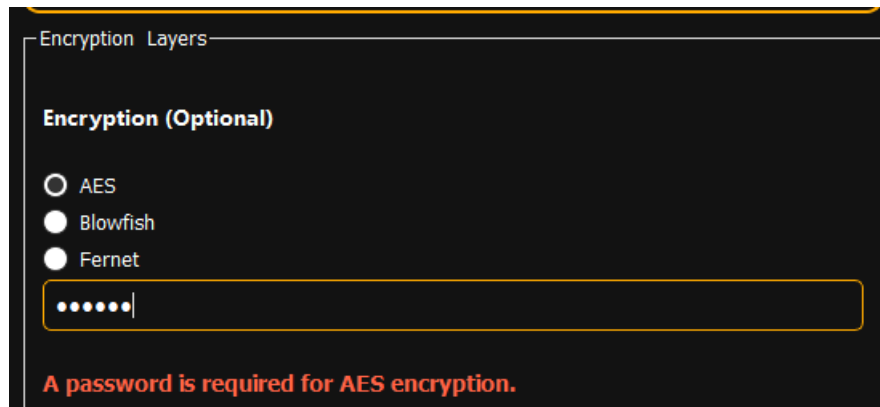


Figure 5 Encryption Layer Panel

Encryption Type selection and password entry for genuine payload. Users must select the primary encryption algorithm for encrypt genuine payload (AES, Blowfish, or Fernet). User also need to enter a password. The password has no requirements so users can enter any password they desire.

6 – Generate Key

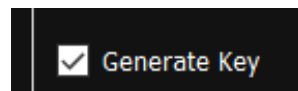


Figure 6 Generate Key Option

Option to generate key **(Optional)**. If user selects the option, Rygelock will create a 'real_key.key' file that is cryptographically tied to user's specific genuine payload.

Before any encryption, Rygelock calculates a SHA-256 hash of raw genuine payload data. This hash is cryptographically stored inside the key file. During extraction, Rygelock will not succeed extracting genuine payload unless the provided key file selected in the extraction panel.

This makes the key file a mandatory second factor for extraction, proving ownership of the original secret data.

7 – Generate Key

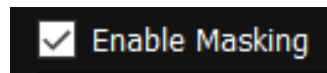


Figure 7 Enable Masking Option

Option to mask genuine payload **(Optional)**. If user selects the option, the encrypted genuine payload will mask before proceeding with steganography operation.

After the genuine payload is encrypted or multi-layer encrypted, this option applies to a high-speed ChaCha20 stream cipher to scramble the ciphertext. The key for this layer is derived from user's password but uses a unique salt and random one-time use nonce, making it independent of the primary encryption keys. This makes the encrypted data even harder to analyze for cryptographic patterns.

8 – Matryoshka Layer (Multi-layer Encryption)

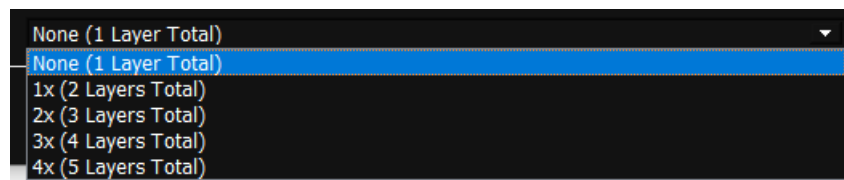


Figure 8 Matryoshka Layer (Multi-layer Encryption) Option

Drop-down list to apply multi-layer encryption to genuine payload **(Optional)**. If user selects any options from the drop-down list (except for “None (1 layer Total)”) Rygelock applies multiple, independent layers of encryption to the genuine payload.

LIST OPTIONS	MEANING
None (1 Layer Total)	No multi-layer encryption. Only single layer encryption applied (Earlier chosen encryption as per Figure 5).
1x (2 Layer Total)	Adds additional layer of encryption to genuine payload (1 additional layer + earlier chosen encryption as per Figure 5).
2x (3 Layer Total)	Adds 2 additional layers of encryption to genuine payload (2 additional layers + earlier chosen encryption as per Figure 5).
3x (4 Layer Total)	Adds 3 additional layers of encryption to genuine payload (3 additional layers + earlier chosen encryption as per Figure 5).
4x (5 Layer Total)	Adds 4 additional layers of encryption to genuine payload (4 additional layers + earlier chosen encryption as per Figure 5).

For each extra layer selected (1x to 4x), Rygelock uses HKDF to derive a new, unique encryption key from your master password and a unique salt for that layer. It then re-encrypts the ciphertext from the previous layer with this new key. This creates a nested-doll style of encryption where an attacker would need to break multiple, distinct cryptographic layers.

9 – Deception Mechanism

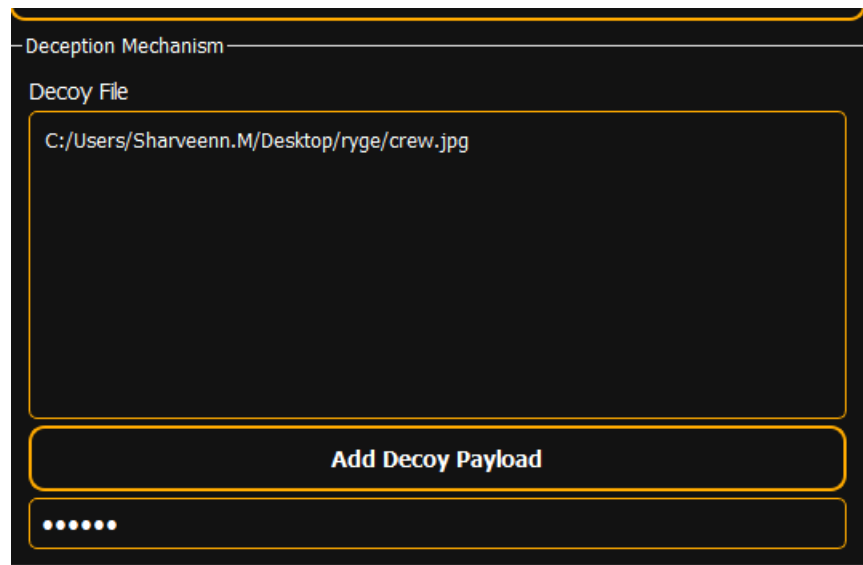


Figure 9 Decoy File with Password

To hide both a genuine payload and a harmless decoy payload in the same carrier file **(Optional)**. If users are forced to reveal hidden content, users can provide the fake password, which will successfully extract the harmless decoy file, protecting the genuine payload stay secret.

Users can only upload one file as decoy file and must provide a password for it. Any type of file can be accepted as decoy file.

10 – Start Hiding Button

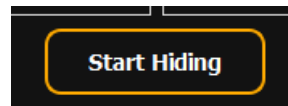


Figure 10 Start Hiding

Button to start steganography operation. When users click the button, Rygelock initiates the steganography process. Rygelock will:

1. Validate all inputs (Check for required passwords, ensure payload size is reasonable).
2. Create the Secure Envelope(s) with all selected security layers.
3. Call the appropriate steganography algorithm to hide the final data inside the carrier.
4. Save the final stego file to the "Rygelock_Output" folder on user Desktop

3.3 Unhide Panel

The screenshot shows the 'Extraction/Unhide Panel' with the following elements and numbered callouts:

- 1**: A 'Back' button in the top left corner.
- 2**: A circular 'Reset' button in the top right corner.
- Carrier File(s)**: A label above the first input field.
- Key File (Optional)**: A label above the second input field.
- 3**: A 'Browse Stego File' button below the Carrier File(s) input field.
- 4**: An 'Upload .key file' button below the Key File (Optional) input field.
- Password (Optional)**: A label above the password input field.
- 5**: An 'Extract' button below the password input field.
- Status:**: A label above the status output area.
- 6**: A large rectangular area at the bottom for displaying the status.

Figure 11 Extraction/Unhide Panel

1 – Back Button

Button to get back to main menu.

2 – Reset Button

Button to reset entire Unhide Panel.

3 – Browse Stego File

This close-up shows the 'Carrier File(s)' section. The input field contains the file path: `C:/Users/Sharveenn.M/Desktop/Rygelock_Output/test.jpg`. Below the input field is a button labeled 'Browse Stego File'.

Figure 12 Upload Stego File

To upload stego file that needs extraction. Users can click the **Browse Stego File** button to browse and load Rygelock stego file.

4 – Upload Key File

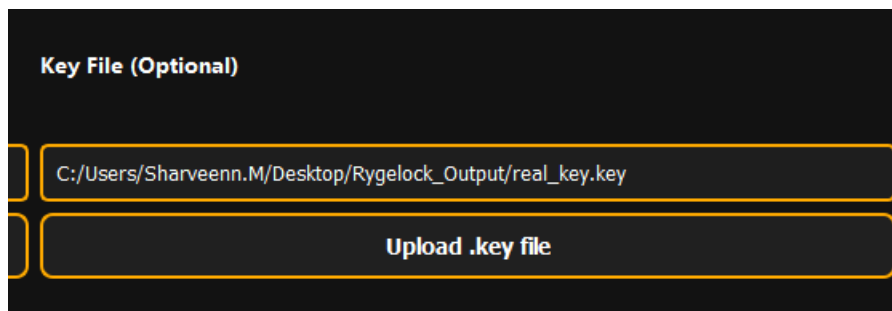
The screenshot shows a dark-themed interface with a label 'Key File (Optional)' in white. Below the label is a text input field containing the file path 'C:/Users/Sharveenn.M/Desktop/Rygelock_Output/real_key.key'. To the left of the input field is a small yellow square icon. Below the input field is a large yellow button with the text 'Upload .key file' in black.

Figure 13 Upload Key File

To load key file that need genuine payload extraction (**optional**). Users can click the **Upload .key file** and load the key file that created with the loaded stego file.

5 – Password for Extraction

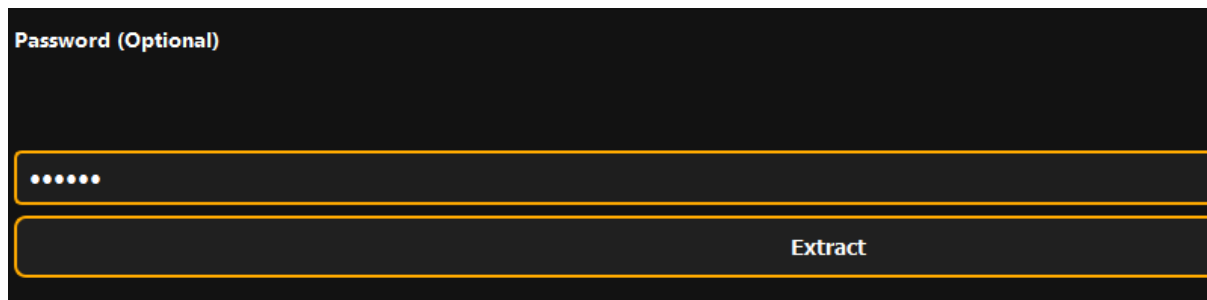
The screenshot shows a dark-themed interface with a label 'Password (Optional)' in white. Below the label is a password input field with six dots. To the left of the input field is a small yellow square icon. Below the input field is a large yellow button with the text 'Extract' in black.

Figure 14 Password for Extraction

User can enter either the password for genuine or decoy payload.

Then click the **Extract** button to start the extraction.

6 – Status Output

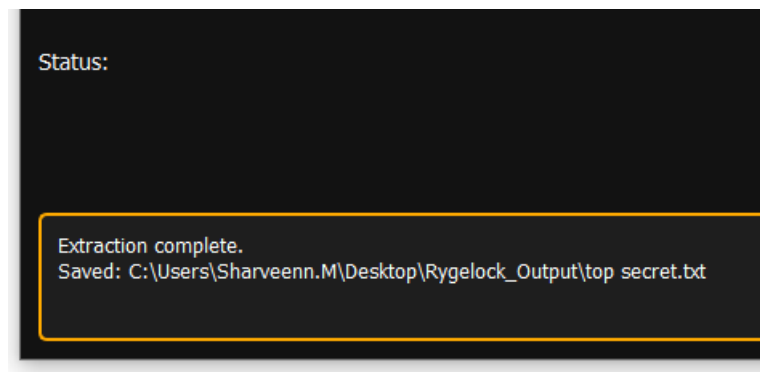


Figure 15 Successful Extraction Status

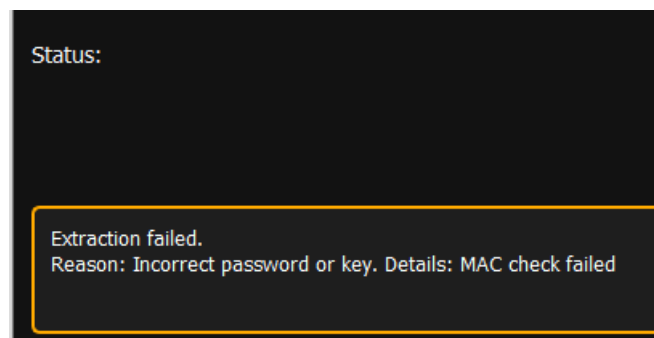


Figure 16 Failed Extraction Status

Users will get successful extraction status output if the correct credentials are given. Users will encounter fail extraction output if wrong stego file is damaged or invalid credentials are given. The status will not indicate anything about genuine or decoy payload. All status output will be generic.

3.4 Rygelock_Output Contents

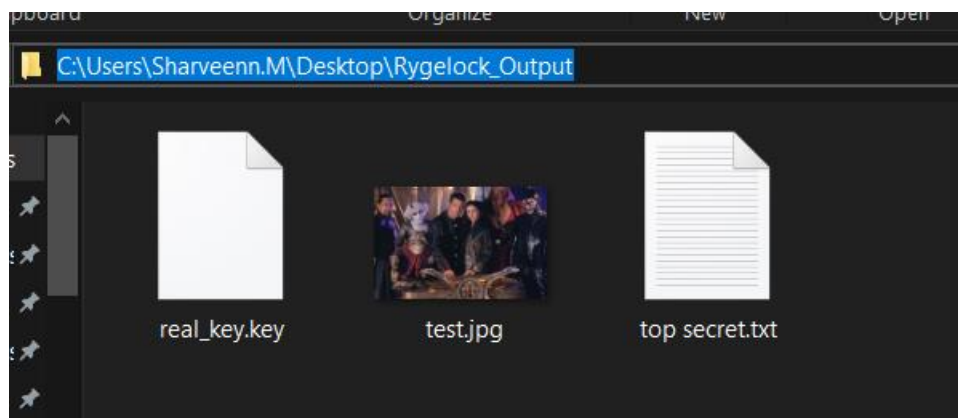


Figure 17 Rygelock Output

After a successful steganography operation and extraction, the stego file, key file (if Generate Key option is selected) genuine and decoy payload (after successful extraction validation) will be saved in a folder called “Rygelock_Output”. The folder will be created by Rygelock in the users’ Desktop. The stego file and payload files will have the same name as the loaded carrier file and payload files in Hide menu.

The selected carrier file, genuine and decoy payload will not be overwritten. Instead Rygelock will copy the files with the exact properties and work on it. Users can rename the stego file and key file as per their desire.

3.5 Settings Panel

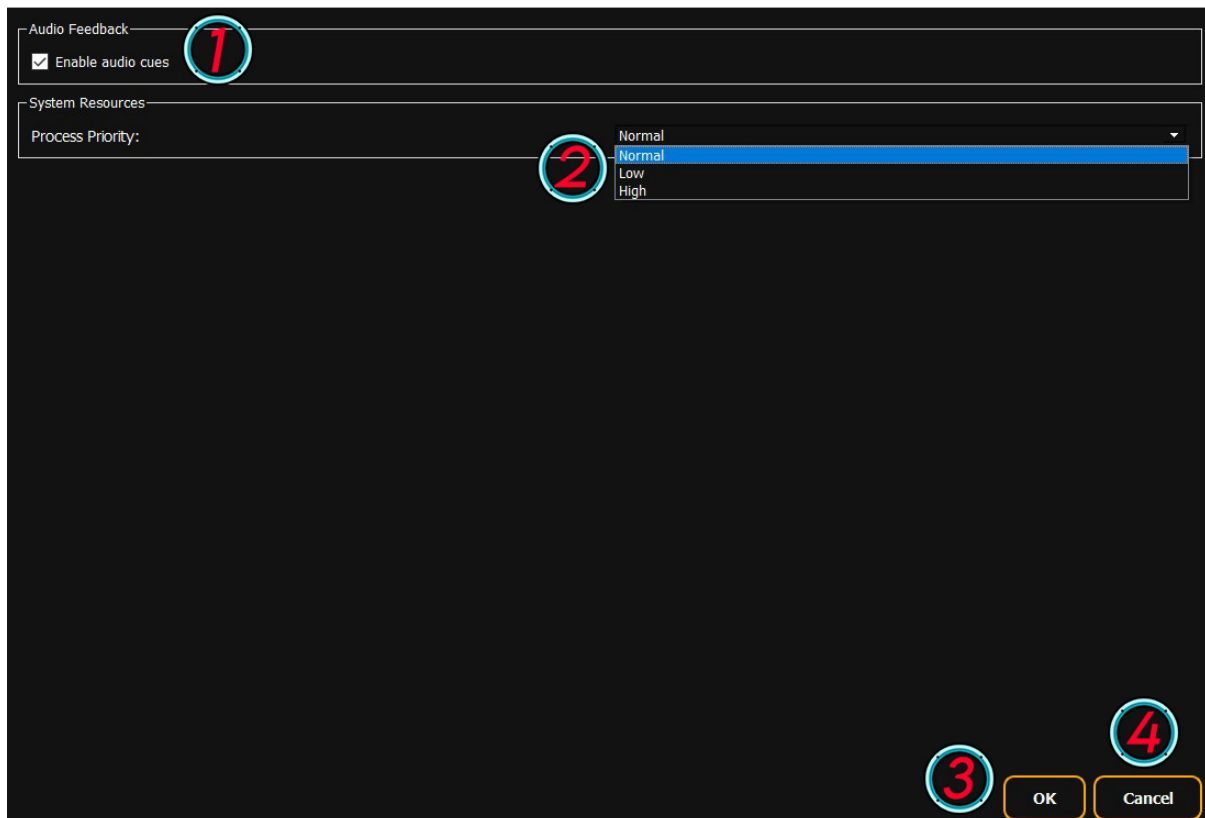


Figure 18 Rygelock Settings Panel

1 – Enable / Disable Audio Cues

Checkbox for mute and unmute. Users can click the checkbox to disable and enable all system audio.

2 – System Resources Allocation

Select CPU resources usage. Users can select the CPU usage for Rygelock.

PROCESS PRIORITY	MEANING
Normal	Uses regular CPU resources.
Low	Only uses CPU resources when any available
High	Will use the highest CPU resources for every Rygelock process than any other process running in users' system

Table 2 Process Priority

3 – Save Changes

Users can click the **OK** button to save any changes in the settings and redirect them to main menu.

4 – Cancel Changes

Users can click the **Cancel** button to discard any changes in the settings and redirect them to main menu.

Default settings are:

Audio Feedback	Enabled
System Resources	Normal

Table 3 Default Settings

The settings are session based. Settings will be always in default when reopening the Rygelock.

4. File Support & Tips

Supported Carriers: PNG, JPG, BMP, TIFF, MP3, MP4

Payload: any file type.

Capacity heuristics: try to keep total payload $\leq \sim 50\%$ of carrier size (images especially) to avoid any distortion or anomalies of steganography.

Matryoshka: prefer fewer layers with a larger carrier over many layers with a tiny carrier.

5. Troubleshooting

“Stego file not created”

- Carrier too small or too compressed; choose a larger/less-compressed file.
- Reduce Matryoshka layers or disable Masking.

“Wrong password/key” or “Decryption failed”

- Ensure you enter the exact Password and the correct .key (if generated).

6. FAQ

Q: Can I use the same password for decoy and genuine?

A: No. You must use different passwords.

Q: Do I always need a key file?

A: Only if you check Generate Key option. If generated, it's required for genuine payload extraction.

Q: Does Masking always help?

A: It improves obfuscation in some carriers. Test with your content.

Q4: What happens if the stego file is modified after embedding?

A: Any significant modification (cropping an image, trimming a video, re-compression, etc.) can corrupt or destroy the hidden payload. For reliable retrieval, the stego file should remain unaltered after embedding.