# Article information:

Binary-block embedding for reversible data hiding in encrypted images - ScienceDirect
<https://www.sciencedirect.com/science/article/abs/pii/S0165168416302742?via%3Dihub>

# Article summary:

1. Binary-block embedding (BBE) method is introduced to embed secret data in a binary image.

2. BBE-RDHEI algorithm proposed for reversible data hiding in encrypted images, with bit-level scrambling process and security key design mechanism to enhance security level.

3. Experiments show that BBE-RDHEI has an embedding rate nearly twice larger than the state-of-the-art algorithms, generates marked decrypted images with high quality, and is able to withstand various attacks.

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

The article provides a detailed overview of the Binary-block embedding (BBE) method for reversible data hiding in encrypted images, as well as the BBE-RDHEI algorithm proposed for this purpose. The article is written in a clear and concise manner, providing sufficient detail on the methods used and their results. The authors provide evidence for their claims through experiments and comparisons with existing algorithms, which demonstrates the reliability of their findings. Furthermore, they discuss potential risks associated with their approach such as brute force attacks, differential attacks, noise attacks and data loss attacks, which shows that they have considered all possible scenarios when designing their algorithm.

However, there are some points of consideration that are not explored in the article. For example, it does not discuss how secure the encryption used is or how difficult it would be to break it using brute force or other methods. Additionally, while the authors do mention potential risks associated with their approach, they do not provide any solutions or strategies for mitigating these risks. Finally, while the authors provide evidence for their claims through experiments and comparisons with existing algorithms, they do not explore any counterarguments or alternative approaches that could be taken when designing a similar system.

# Topics for further research:

* Encryption security
* Brute force attack prevention
* Differential attack prevention
* Noise attack prevention
* Data loss attack prevention
* Alternative approaches for reversible data hiding

# Report location:

<https://www.fullpicture.app/item/69fb1d5b67ad5c9365794c53b8e10751>