# Article information:

Automatic Classifier Based Reversible Image Transformation for Reversible Data Hiding in Encrypted Images | IEEE Conference Publication | IEEE Xplore
<https://ieeexplore.ieee.org/document/8663124>

# Article summary:

1. Cloud computing is popular for storing multimedia information, but the cloud server cannot embed data inside client images without a reversible data hiding approach.

2. Reversible image transformation and reversible data hiding can be used in forensics, military, and medical imagery where the encoded and decoded image should remain the same.

3. Various approaches have been introduced for reversible data hiding in encrypted images, including histogram shifting, prediction-based embedding, and frequency domain transformations like DCT, FFT, and DWT are not applicable because they are mostly lossy.

# Article rating:

Appears strongly imbalanced: The article is written in a biased or one-sided way, and the information it provides is not trustworthy enough to be considered a reliable source. You should consult other sources to find reliable information on the presented issues.

# Article analysis:

The article titled "Automatic Classifier Based Reversible Image Transformation for Reversible Data Hiding in Encrypted Images" discusses the need for reversible data hiding in encrypted images and proposes an approach based on automatic classification. While the article provides some useful information, it has several limitations that need to be addressed.

One of the potential biases in the article is its focus on cloud computing as the primary use case for reversible data hiding. While cloud computing is undoubtedly a significant application area, there are many other scenarios where reversible data hiding can be useful, such as digital forensics, steganography, and watermarking. By limiting the discussion to cloud computing, the article may miss out on other important use cases.

Another limitation of the article is its one-sided reporting of existing approaches to reversible data hiding. The authors only mention a few techniques based on histogram shifting and prediction errors but do not provide a comprehensive overview of all available methods. This omission may lead readers to believe that these two approaches are the only viable options when there are many others worth considering.

The article also makes unsupported claims about the limitations of frequency domain transformations like DCT, FFT, and DWT. The authors state that these transformations are mostly lossy and hence not reversible without providing any evidence to support this claim. In reality, there are many lossless frequency domain transformations that can be used for reversible data hiding.

Moreover, the article does not explore counterarguments or potential risks associated with their proposed approach. For example, it is unclear how well their automatic classifier performs on different types of images or how robust it is against attacks aimed at breaking the encryption or extracting hidden data.

Finally, there is some promotional content in the article that may bias readers towards their proposed approach. For instance, they claim that their method outperforms existing techniques without providing any empirical evidence to support this assertion.

In conclusion, while the article provides some valuable insights into reversible data hiding in encrypted images using automatic classification-based transformation, it has several limitations that need to be addressed before accepting its claims at face value. Readers should critically evaluate its content and consider alternative approaches before making any decisions about which technique to use for their specific application scenario.

# Topics for further research:

* Reversible data hiding techniques beyond histogram shifting and prediction errors
* Lossless frequency domain transformations for reversible data hiding
* Risks and limitations of automatic classification-based transformation for reversible data hiding
* Robustness of reversible data hiding techniques against attacks on encryption and data extraction
* Applications of reversible data hiding beyond cloud computing
* Empirical evidence comparing the performance of different reversible data hiding techniques.

# Report location:

<https://www.fullpicture.app/item/0f3e4c5e9528dfcf6e56207c4691a196>