**A NEW RULE FOR COST REASSIGNMENT IN ADAPTIVE STEGANOGRAPHY**

**ABSTRACT**

In steganography schemes, the distortion feature is used to outline modification prices on cover elements that are exceedingly vital to the security of contemporary adaptive steganography. There are several successful rules for reassigning the prices described by using a given distortion feature, which could promote the security stage of the corresponding steganographic algorithm. on this paper, we suggest a novel value reassignment rule that's implemented to no longer one but a batch of present distortion functions. we discover that the costs assigned on a few pixels by means of numerous steganographic strategies may be very distinct even though those strategies show off close security levels. We name such pixels “controversial pixel”. Experimental effects display that steganalysis capabilities are not touchy to arguable pixels; therefore these pixels are appropriate to hold extra payloads. We name this rule the controversial Pixels earlier (CPP) rule. Following the rule of thumb, we recommend a price reassignment scheme. Thru sizeable experiments on several types of stego algorithms, steganalysis features and cowl databases; we exhibit that the CPP rule can improve the security of state-of-the-art steganographic algorithms for spatial photographs.

|  |  |
| --- | --- |
| **EXISTING SYSTEM** | **PROPOSED SYSTEM** |
| **EXISTING CONCEPT:-**   * Most modern secure image steganographic schemes define distortion functions for constraining the embedding changes to those parts of the image that are difficult to model such as textured or noisy regions. * We present a two-player zero-sum game between steganographer and attacker related to the security of practical steganography | **PROPOSED CONCEPT:-**   * The distortion function is used to define modification costs on cover elements, which is distinctly vital to the security of modern adaptive steganography. * There are several successful rules for reassigning the costs defined by a given distortion function, which can promote the security level of the corresponding steganographic algorithm. |
| **EXISTING TECHNIQUE:-**   * UNIWARD (Spatial-UNIversal Wavelet Relative Distortion) | **PROPOSED TECHNIQUE:-**   * Controversial Pixels Prior (CPP) rule. |
| **TECHNIQUE DEFINITION:-**   * The CPP rule considers a combination of several existing methods instead of remaining fixed on a single method. * An essential principle in selecting candidate algorithms for the CPP rule is that basic methods have comparable security performances. In addition, the CPP rule provides a novel tool for designing steganographic schemes. | **TECHNIQUE DEFINITION:-**   * Proposed the algorithm which assigns high costs to pixels that are more predictable by a bank of directional filters. * It defines distortion functions by investigating how to reasonably define the complex degrees of pixels in the sense of resisting detection. The core idea of *Complexity Prior*, several effective rules for ranking priority of pixels have been proposed by previous works |
| **DRAWBACKS:-**   * Moderate distortion * Noise is high | **ADVANTAGES:-**   * Noise reduction * Improved distortion |

**SOFTWARE REQUIREMENT**

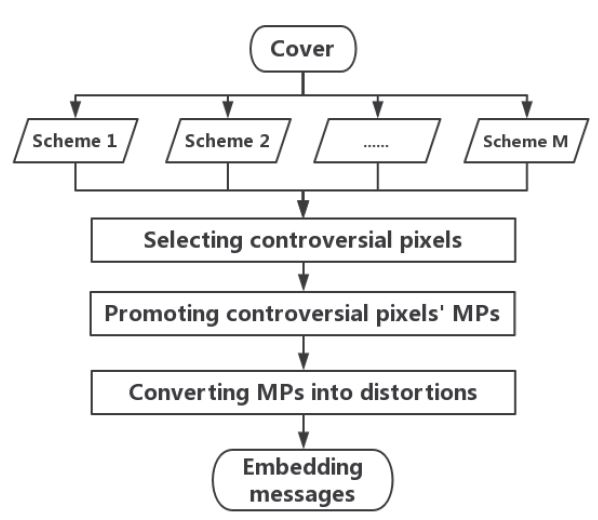
* Operating system :- Windows7(with service pack1),8,8.1 and 10
* Front End :- Microsoft Visual Studio .Net 2013
* Coding Language :- C#
* Backend :- SQL Server 2012

**HARDWARE REQUIREMENT**

* Processor : Pentium Dual Core 2.00GHZ
* Hard disk : 120 GB
* Mouse : Logitech.
* RAM : 2GB(minimum)
* Keyboard : 110 keys enhanced

|  |  |
| --- | --- |
| **PROPOSED SYSTEM** | **FUTURE ENHANCEMENT** |
| **PROPOSED CONCEPT:-**   * The distortion function is used to define modification costs on cover elements, which is distinctly vital to the security of modern adaptive steganography. * There are several successful rules for reassigning the costs defined by a given distortion function, which can promote the security level of the corresponding steganographic algorithm. | **FUTURE CONCEPT:-**   * The proposed framework reduces the design of secure steganography in empirical covers to the problem of finding local potentials for the distortion function that correlate with statistical detectability in practice. * By working out the proposed methodology in detail for a specific choice of the distortion function, we experimentally validate the approach and discuss various options available to the steganographer in practice. |
| **PROPOSED TECHNIQUE:-**   * Controversial Pixels Prior (CPP) rule. | **FUTURE ALOGRITHM:-**   * Current model-preserving (CMP) steganographic |
| **TECHNIQUE DEFINITION:-**   * Proposed the algorithm which assigns high costs to pixels that are more predictable by a bank of directional filters. * It defines distortion functions by investigating how to reasonably define the complex degrees of pixels in the sense of resisting detection. The core idea of *Complexity Prior*, several effective rules for ranking priority of pixels have been proposed by previous works | **TECHNIQUE DEFINITION:-**   * We make a connection between steganography design by minimizing embedding distortion and statistical physics. * The unique aspect of this work and one that distinguishes it from prior art is that we allow the distortion function to be arbitrary, which permits us to consider spatially dependent embedding changes. We provide a complete theoretical framework and describe practical tools, such as the thermodynamic integration for computing the rate-distortion bound |
| **ENRICHMENT:-**   * Noise reduction * Improved distortion rate | **EXTRAVAGANCE:-**   * Thermodynamic integration. * Rate-distortion bound. |

**SYSTEM ARCHITECTURE**

****