A Filter Parametric Control Approach to Embedding Capacity in Adaptive Steganography*

Atul Negi\textsuperscript{1} and N Santosh Arjun\textsuperscript{2}
\textsuperscript{1}Department of CIS, University of Hyderabad, Hyderabad, India – 500 046.
\texttt{atul.negi@ieee.org}
\textsuperscript{2}Department of ECE, University College of Engineering (A), Osmania University, Hyderabad, India – 500007.
\texttt{santosharjun@ieee.org}

*This is an extended and expanded version of the paper published in the SWAN 2006 workshop, IEEE International Conference on Digital Information Management, Bangalore India pp 525-530, December 6-8\textsuperscript{th} 2006. See references [14] in this paper.

Abstract: Adaptive steganography comes closer to the ideal of steganography since it exploits the natural variations in the pixel intensities of a cover image to better hide the secret message. Most of the adaptive steganographic methods in the literature use local features of an image for embedding the message, which are easily attacked. In this paper a new method of adaptive steganography is proposed, that uses both global and local image features. The novel approach uses a digital filtering and embedding process that allows for a high embedding capacity and enhanced security. The proposed approach through the filter design controls parametrically the embedding of information into the cover media. A detailed algorithm is presented in this paper with results of extensive experimentation on a large number of sample images shows a much higher embedding capacity. A comparison of stegano-analytic features of existing adaptive steganographic methods and the new method are also presented. We believe this approach shall improve the secrecy of communication of images and lead to better digital information management.

Keywords: Steganography, Filtering, Digital Watermarks, Image Confidentiality.

1. Introduction

The secrecy of obviously encrypted digital information sent across an open communication medium like the internet is always questionable. Cipher text naturally attracts suspicion and due to the availability of computation power breaking the cipher-text codes is now quite possible. To enhance message secrecy it may better to exploit a recent phenomenon of the internet where increasingly larger information is available in a non-textual or visual imagery format and it is possible to hide information using steganography. With steganography imperceptibility is important and it is preferred to have an adaptive process that allows hiding of data within another information stream called as cover media. To improve the imperceptibility the adaptive process should attempt to make use of the specific characteristics of that media. This adaptation is what makes it apparently innocuous. Suitable cover media for adaptive steganography are any digital media that have redundant or perceptually irrelevant information such as images, audio, video etc. [19]. Steganography essentially is a multi-disciplinary field combining use of image and signal processing techniques with cryptography, communication theory, coding theory, signal compression theory of visual perception, etc [16]. Here we propose an approach that parametrically (through the filtering process) controls the embedding of information into the cover media. We study several aspects of this simple but novel approach to adaptive steganography.

We now review the essential functional components of a basic adaptive steganographic system that is used to describe our proposed approach. The basic steganographic model is shown in Figure 1. Consider that a transmitter consists of a cover image $C$ (which acts as a carrier), and the message $M$ is the data that a sender wishes to communicate confidentially. $M$ can be plain/cipher text, images, or anything that can be embedded in a bit stream. The cover image $C$ is used to embed the message by using a stego-encoder controlled by stego-key $K$. $K$ is a shared secret with the intended recipient whose knowledge of the key enables them to decode the message from $M$.

![Figure 1: Basic Steganographic Model.](image-url)
Steganalysis is a process of discovering the presence of information that can be hidden in a given cover image. In this paper we present a parametric approach where a digital filter and its design parameters provide the stego-key. The decoding parameters are understood to be known to both sender and receiver and are referred to as a shared secret. In this paper our main concern is in explaining the steganographic technique, how such shared secrets are communicated confidentially is outside the scope of this paper. The resulting stego-image obtained after embedding information is represented as \( S = f(C, M, K) \). \( S \) is transmitted over a channel to the receiver where it is processed by the stego-decoder using the same key \( K \). An interceptor of the stego-image is expected to only see the innocuous image without any obvious indication of the embedded hidden message. Recovering the hidden message \( M \) from a stego-image requires the cover-image \( C \) itself and the corresponding decoding key \( K \). The original image may or may not be required in most applications to extract the message at the receiver.

Steganography and cryptography are cousins in the spycraft family [1]. For most practical purposes data that is to be embedded in cover media can be encrypted before applying steganographic (stego) methods, thus allowing an additional level of security. Some of the applications of steganography are in covert and military communications, commercial and anti-criminal related applications [21].

Steganographic methods are evaluated based on their information hiding capacity and imperceptibility. There is always a trade-off between the invisibility and the amount of information that can be hidden in a given cover image. Steganalysis is a process of discovering the presence of steganography using the difference in statistical features of a cover and stego-image. A given steganographic method is said to be secure if the stego-image produced using that method does not contain any detectable artifacts due to message embedding [8]. In other words, given the knowledge of the embedding algorithm and the source of cover media, the attacker shouldn’t be able to distinguish between stego and cover objects with a success rate better than random guessing [20]. When the presence of stego content is suspected the main goal of steganography is defeated [12], since an attacker may attempt to block the communication of the message or attempt to change/obliterate the embedded message. More sophisticated attacks might decode the message. So, as to maintain the maximum similarity between stego and cover media, the obvious solution is to embed less amount of information into the cover media, so that the probability of introducing detectable artifacts by the embedding process is smaller [8]. However the goal of an effective steganographic method would be to maximize the amount of hidden information that can be communicated, while ensuring that the cover media is minimally distorted.

In this paper, our approach aims to reduce the risk of detection while keeping a high embedding capacity. Adaptive steganography attempts to secure greater stealth for the message by ensuring that the changes introduced into the cover image remain consistent with the natural noise model associated with cover images. Even if our method is known in principle, the secrecy of the hidden data is derived from the relatively large computational cost needed to find the digital filter parameters. Further the filter parameter value in our proposed approach also acts as a control parameter that varies the embedding capacity, which was not seen in previous approaches to adaptive steganography. In a later section of the paper we also show that the decoding of the message information is very specific (selective) to the parameter value so that random guessing is unlikely to break it.

In section II we review some of the existing adaptive steganographic methods. In section III the basis for our new method and its implementation is presented, followed by the algorithm and results. In section V a comparison between existing steganographic methods and the new method are presented.

## 2. Existing Adaptive Steganographic Methods.

Here we review a progression of the adaptive steganographic methods and how they were strengthened against attacks. An older and very widely used steganographic method is the Least Significant Bit (LSB) steganographic method. In this method one replaces the LSB bits of an image with the message or data bits to be transmitted. The problem with this method is that when we use a greater number of LSB’s i.e. 3 or 4 LSBs for message embedding, some visible signatures are left on the image. When only 1 or 2 LSBs are used, steganographic content can be found by visual attacks [8] (a visual attack means that the LSB planes used for steganography overwrite the visual structures of the cover image). \( JSteg \) [17-18] is a transform domain based approach was proposed so as to resist visual attacks. It replaces the least significant bits of DCT (Discrete Cosine Transform) coefficients with the message’s data. Westfeld and Pfitzmann [8] proposed a \( \chi^2 \)-attack which can detect the presence of steganographic content in a stego-image where message data is embedded sequentially. The approach known as Outguess [17] embeds data in a pseudo-random manner, so as to remain undetected. However RS-Steganalysis [9] can detect the presence of steganography in stego-images, even though the messages are embedded in a random manner.

So as to overcome these deficiencies adaptive steganography was proposed which aims to reduce modifications to the cover image, and adapt the message embedding technique to the actual content and features of the cover image. Adaptive methods embed a message bit into certain random clusters of pixels, avoiding areas of uniform color and select pixels with large local standard deviation or blocks containing a number of different colors. Invisibility is relative to the sensitivity of the human visual system and is attained by altering the cover image accordingly. Various statistical parameters [13] used by steganalysis algorithms are also to be kept in mind when creating the stego-image. The major challenge posed in using
existing adaptive steganography techniques is that the methods do not seem to allow any parametric control on the quantum of information that is to be embedded, for a given cover image. This problem is overcome in the method presented in this paper. We take a brief look at some of the existing adaptive steganographic methods before proposing ours.

One of the adaptive approaches proposed by Chandramouli et al. [4] assumes that the sender is aware of the steganalyzer used by a stegan-attacker and the sender needs to adapt the embedding algorithm accordingly to avoid detection. It is quite clear that such an assumption is quite restrictive, unreasonable and impractical.

The method StegoAdapt [5] was implemented based on the adaptive method described in [22]. In this method the cover image is divided into 3x3 blocks of pixels, and the message bit is encoded as the parity of the central pixel in each pseudo randomly selected potential block. The block is considered to be suitable for bit storage if, the central pixel in the block is different as compared to at least one of the surrounding pixels in the block. A suitable block may become unsuitable after bit storage so it is checked again after embedding. The search for a suitable block continues ahead into the image, skipping those blocks which become unsuitable after embedding. When the message is read from the image, only the bits from the suitable blocks are combined to reassemble the message. This method doesn’t leave any visible signatures of steganographic content but, the embedding capacity of this approach is easily found to be at best the number of pixels in the image divided by 9, which is clearly insufficient for many practical purposes.

In another method known as AdMod, the embedding function is chosen depending on a dither mask [6], which should be parameterized for most practical purposes such that the embedding function is adapted to the image content. In this method, in order to complicate histogram analysis, we either increment or decrement the pixel values instead of LSB replacement. Random selection of sequence of pixels can be used so that small messages are spread over the cover image. While this method provides a higher embedding capacity as compared to StegoAdapt it is prone to visual and $\chi^2$ attacks.

In another method known as ConDith [6] a message is adaptively embedded into a cover image based upon a contrast dithering process. This attempts to improve over AdMod where image intensity is used for message embedding and where existing image structures may be destroyed after message embedding. Thus ConDith uses local contrast of an image as a dithering criterion. Only those regions showing a high degree of variation in contrast are selected for the dither criterion for embedding. In the dithering algorithm the pixel differences to immediate neighbors are compared to a threshold value of minimum contrast $C_{\text{min}}$. A pixel is used steganographically, if the contrast difference exceeds $C_{\text{min}}$ otherwise it is not usable. Only if the difference between the pixel and each of its neighbors exceeds the threshold value then it is used for embedding. The sum of differences is not used in order to avoid irregularities e.g. at the edges.

The adaptive steganographic methods discussed above satisfy the constraint of adapting the embedding process to the content of the cover image. However, they do not have a high embedding capacity. Further we have no parametric control over the embedding capacity. In the next section we propose a method which provides a parametric control over the embedding capacity and also adapts the embedding process to the content of the cover image. We also show that our proposed method is resistant to some well known steganalytic attacks.


The proposed approach utilizes the weakness of the human visual system and adaptively modifies the intensities of pixels obtained after filtering. These are the high frequency components spatial image pixels (HFSI) of the cover image. The modification of pixel intensities depends on the magnitude of the pixels in HFSI and also on the local features of the cover image. If the contrast of the image is large (e.g., at an edge), the intensities can be changed greatly without introducing any distortion to human eyes. On the other hand, if the contrast is small (e.g., a smooth image), the intensities can only be tuned slightly.

First, we pass the cover image through a filter to separate the high and low frequency components of the image. The inverse transform of both the images is computed. Now the pixels values of HFSI are modified depending on the magnitude of the pixel. If the magnitude of the LSBS of a pixel is large then a larger number of LSBS can be modified to embed the stego information. This approach is also adaptive to the local features of the cover image. Now both the LFSI (Low Frequency components spatial image of cover image) and HFSI are added to form the stego-image. At the receiver the reverse process is to be done to recover the message.

A. Algorithm

Step 1: Let the cover image be represented by $c(x,y)$. It is then passed through a filter with transfer function $h(x,y)$ to separate high and low frequency components. The filter has a threshold cutoff frequency of $\theta$.

$$F[c(x,y)] = C(X,Y)$$  \hspace{1cm} - (1)

Where $C(X,Y)$ represents Fourier Transform of the cover image (we use upper case letters for frequency domain and lower case letters for spatial representation).

$$C(X,Y)H(X,Y) = LO(X,Y) + HI(X,Y)$$  \hspace{1cm} - (2)

Where $LO(X,Y)$, $HI(X,Y)$ represent low frequency and high frequency components of cover image respectively, obtained after passing through the filter with cut off as stated above.

Step 2: Inverse transform of both the frequency components is found out, known as HFSI and LFSI separately.

$$F^{-1}[LO(X,Y)] = lo(x,y)$$  \hspace{1cm} - (3)
where $l_0(x,y)$ and $h_1(x,y)$ are the spatial components of low and high frequencies in the cover image, respectively.

Step 3: Now the message is embedded into HFSI image. The number of bits modified in a pixel depends upon its magnitude and also upon the local features of the cover image. If the message is $m(x,y)$ and the embedding function is $M[f]$ (the details of the embedding function $M[f]$ are taken up in the next section) then

$$mhi(x,y) = M[hi(x,y) + m(x,y)]$$  \hspace{1cm} (5)

Step 4: Both the modified HFSI and unmodified LFSI are added to form stego-image.

$$steg(x,y) = mhi(x,y) + l0(x,y)$$  \hspace{1cm} (6)

Step 5: At the receiver LFSI image is subtracted from stego-image leaving modified HFSI image.

$$mhi(x,y) = steg(x,y) - lo(x,y)$$  \hspace{1cm} (7)

Step 6: Now the message is decoded from the Modified HFSI image using the stego-key.

$$m(x,y) + hi(x,y) = M^{-1}[mhi(x,y)]$$  \hspace{1cm} (8)

B. Example Application of Algorithm

The cover image selected is Petronas Towers image with a pixel size of 300×200 pixels. This image is given in figure 2(a). The figure 2(b) is obtained when the cover image is passed through a Gaussian, 2-D FIR low pass filter with normalized cut-off frequency 0.351 and order 23. This image is the LFSI image $l_0(x,y)$, as explained. The figure 2(c) is obtained by subtracting figure 2(b) from figure 2(a), and is the HFSI image $h_i(x,y)$ given by

$$hi(x,y) = c(x,y) - lo(x,y)$$  \hspace{1cm} (9)

1) Adaptive Embedding Based on Pixel Magnitude in Filtered Image and Local Features of a Cover Image.

In this section we show how the HFSI image is modified, by embedding the message using the function $M[f]$. This modifies the lowest K-2 bits of the HFSI image according to the magnitude at $hi(x,y)$, and also taking into consideration the local features of $c(x,y)$. Although many possibilities exist, for this example we use the following embedding algorithm.

Step 1: First a 3×3 block is moved over the cover image centered at location $(x,y)$. If all the pixel values under the block in $c(x,y)$ are the same, then the central pixel of the block in $hi(x,y)$ is not used for message embedding. All the remaining pixels of $hi(x,y)$ are modified in the following way.

Step 2: For a given pixel in $hi(x,y)$, we find the first non-zero MSB bit, which is the $K^{th}$ bit from LSB side as shown in Figure 3. ($K$-2) bits of that pixel are replaced by message bits and $(K-1)^{th}$ bit is modified such that the error between original pixel and the modified pixel value is reduced. For example, if $hi(x,y)$ magnitude is either 2, 3, a single bit (the least significant bit) is replaced by the message bit. The $K^{th}$ bit cannot be used for embedding message information since it is used at the receiver to mark the number of message bits for a given pixel in the stego-image $steg(x,y)$.

For the above algorithm the numbers of bits modified for each magnitude are summarized in Table 1. Using the above scheme for the cover image in Figure 2(a), 580 pixels cannot be used for message embedding, as they are part of a constant color region. From experimentation we find that 122,916 bits
can be modified in the image according to this embedding method. Consider the message image (M) 115×115 pixels in size as shown in Figure 4. After embedding this image into HFSI image (Figure 2(c)), Figure 5(a) is obtained called as Modified HFSI image. The stego-image \(\text{steg}(x,y)\) is formed after adding LFSI image \(\text{lo}(x,y)\) and modified HFSI image \(\text{mhi}(x,y)\) and is shown in Figure 5(b).

\[
\text{steg}(x, y) = \text{mhi}(x, y) + \text{lo}(x, y)
\]

The receiver obtains \(\text{steg}(x,y)\) which was transmitted and already has the cover image \(c(x,y)\) and knows the cut-off frequency \(\theta\), he can compute the low frequency components spatial image of cover image \(\text{lo}(x,y)\). Then \(\text{mhi}(x,y)\) is found as below.

\[
\text{mhi}(x, y) = \text{steg}(x, y) - \text{lo}(x, y)
\]

To decode the message an inverse of the embedding function, \(M^{-1}[]\) is used from which \(\text{hir}(x,y)\) is a residue that is an MSB approximation of \(\text{hi}(x,y)\) and is discarded.

\[
\text{m}(x, y) + \text{hi}(x, y) = M^{-1}[\text{mhi}(x, y)]
\]

### 4. Experimentation and Discussions

In this section we study experimentally the effect of \(\theta\) (cut-off frequency) as the parameter used to control the information hiding capacity. We also compare our approach with others with respect to the embedding capacity and resistance to steganalysis.

<table>
<thead>
<tr>
<th>Table 1. Number of Bits that can be used for hiding information for a given magnitude of a pixel in HFSI Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magnitude of Pixel in HFSI Image (M)</td>
</tr>
<tr>
<td>---------------------------------</td>
</tr>
<tr>
<td>0&lt;=M&lt;2</td>
</tr>
<tr>
<td>2&lt;=M&lt;4</td>
</tr>
<tr>
<td>4&lt;=M&lt;8</td>
</tr>
<tr>
<td>8&lt;=M&lt;16</td>
</tr>
<tr>
<td>16&lt;=M&lt;32</td>
</tr>
<tr>
<td>32&lt;=M&lt;64</td>
</tr>
<tr>
<td>64&lt;=M&lt;128</td>
</tr>
<tr>
<td>128&lt;=M</td>
</tr>
</tbody>
</table>

### A. Comparison of Embedding Rate

The embedding rate denotes the average number of bits that can be embedded per pixel into a given cover image. It depends upon both the stego-algorithm and the cover image content. In our tests a random message of variable length is used so that the arbitrary embedding capacity can be calculated. Embedding rate rather than embedding capacity is considered because embedding rate gives the average number of bits that can be modified per pixel whereas embedding capacity corresponds to the total capacity of a given cover image thus embedding rate is more appropriate to use with images of different sizes. The maximum embedding rates of various adaptive steganographic methods discussed in this paper and the maximum embedding rate of our new method are summarized in Table 2. An embedding rate of 100% corresponds to an embedding rate of 1 bit/pixel. The maximum embedding rate we find is theoretically to be 600% (for the example embedding algorithm of section IV). This is computed by looking up the maximum number of bits/pixel that can be used for information hiding as shown in Table 1 and also by assuming that each pixel of HFSI has a magnitude ≥ 128.

In our experimentation the proposed method and the others were applied upon a wide variety of 72 images which includes common images like Lena, Baboon, Peppers etc., some texture images [24] and natural images [25] and the results were compared. The AdMod method has a comparable embedding capacity but it is relatively susceptible to certain steganalysis programs as mentioned in [6] and also shown in the next subsection. From the Table 2 it is apparent that the proposed method has a higher embedding rate compared to existing methods. It is clear that for any method, there is always a trade-off between amount of message information that can be hidden, and its perceptibility to attacks.

### B. Effect of Cut-Off Frequency on Information Hiding Capacity

<table>
<thead>
<tr>
<th>Table 2. Comparison of Embedding Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Steganographic Method</td>
</tr>
<tr>
<td>---------------------------------</td>
</tr>
<tr>
<td>Maximum</td>
</tr>
<tr>
<td>---------------------------------</td>
</tr>
<tr>
<td>StegoAdapt</td>
</tr>
<tr>
<td>AdMod</td>
</tr>
<tr>
<td>ConDith</td>
</tr>
<tr>
<td>New Method</td>
</tr>
</tbody>
</table>

![Figure 4 Message Image to be hidden in Cover Image](image)
In our approach we use the control parameter $\theta$ so that a user can have a choice about the amount of information to be embedded into a given cover image. This parameter changes the cut-off frequency of the filter. The effects of change in cut-off frequency on the embedding capacity are summarized in the Figure 6. This result is obtained for the example cover image we have shown earlier. From Figure 6, one can easily observe that a variation in information hiding capacity can be obtained by tuning the cut-off frequency $\theta$.

In Figure 7 we see how the embedding rate varies with the normalized threshold for various other images. Here we observe that the form of the curve remains the same although there is some variation in the embedding capacity for the images. This but natural and is expected. Consider Figure 8 where we are concerned with the distortion in the stego-image. Here we observe that for small embedding capacities (less than one) a very high value of PSNR is obtained. However more practical utility is seen from the region of curve where in the PSNR remains flat (almost parallel to the horizontal axis). Here we can see that it is indeed possible to choose a higher embedding capacity for some given (arbitrary) value of image degradation (PSNR value). This curve is very useful practically as it allows a choice or trade-off between secrecy (higher PSNR) and embedding capacity. In Figure 9 we provide another way for the designer to choose a cut-off frequency based upon an arbitrary PSNR value.

C. Resistance to Steganalysis Methods

Steganalysis involves detecting the presence of steganography and if possible, decoding the embedded message, changing it and/or destroying the message to render it useless. Steganalysis is also used to determine whether a message is secure, and consequently whether the steganographic process has been successful [5]. Steganalysis methods examine the patterns produced in the suspected stego-images and look for any tell-tale signatures in detection. The following methods were implemented and applied on the stego-images obtained from our proposed algorithm:

- Visualizing the LSB Planes [8]
- $\chi^2$-attack [8].
- Histogram Analysis

LSB planes are visualized because they are very simple to

\begin{figure}
\centering
\includegraphics[width=0.4\textwidth]{figure6.png}
\caption{Effect of Cut-off Frequency $\theta$ on Embedding Capacity of Hidden Information for the Example explained above.}
\end{figure}

\begin{figure}
\centering
\includegraphics[width=0.4\textwidth]{figure7.png}
\caption{Normalized cut-off frequency vs. embedding rate for some images.}
\end{figure}

\begin{figure}
\centering
\includegraphics[width=0.4\textwidth]{figure8.png}
\caption{Normalized cut-off frequency vs. PSNR ratio.}
\end{figure}

\begin{figure}
\centering
\includegraphics[width=0.4\textwidth]{figure9.png}
\caption{Embedding rate vs. PSNR ratio.}
\end{figure}
understand and also easy to implement. In the literature the two effective and widely used LSB steganalysis methods are RS steganalysis and $\chi^2$-attack. But RS steganalysis is more accurate for messages that are randomly scattered in the stego-image than for messages that are embedded sequentially [9]. For sequentially embedded messages, the method described in [8] is the $\chi^2$ attack is said to be more effective and reliable.

1) **Visualization of LSB planes**

We first visualize LSB planes as embedding of any data will have more effect on LSB planes. A cover image and its original LSB plane are shown in Figure 10(a) and 10(b) respectively. The LSB plane of the stego-image obtained from Figure 10(a) is shown in Figure 10(e). From these figures we can conclude that our method doesn’t seem to have an apparent effect on the LSB plane. This could be attributed to the fact the message is embedded by taking into consideration the local features of the cover image. The corresponding images obtained from the ConDith method and AdMod method are shown in Figures 10(c) and (d). The failure of AdMod is clearly visible.

2) **Analysis of $\chi^2$ attack**

The $\chi^2$ attack is a statistical attack widely used to test steganographic methods especially sequential LSB steganographic methods. Test results are divided into three classes (categories). C1 is the first class where we have cover images for which no differences at all can be computed by the test between cover and stego-images. This includes all images that resist the $\chi^2$-attack. Images in the second class C2 also resist this attack but show no significant differences between cover and stego-images. The images in the third class C3 show significant differences between cover and stego images. The results are summarized in Table 3, where this attack was applied on stego-images produced by the proposed approach. From Table 3 it is clear that adaptive steganography based on filtering is resistant to this attack.

In comparison we refer the reader to the results of this attack using the methods AdMod and ConDith as reported by [6]. We ask, what may be the reason for such a good performance of the proposed approach which has the additional quality of a higher embedding rate? We attribute it to the steganographic process. That is, the modified HFSI image is added to the LFSI image, whose pixels vary in magnitude thus resulting in a stego-image with a wide range of distribution of pixel values. Another property of the stego-image thus produced is that plain regions are avoided for message embedding, thus a statistical approach like the $\chi^2$-attack would not really find anything anomalous.

3) **Histogram Analysis**

The histograms of the cover image $c(x,y)$ and the stego-image $stg(x,y)$ are shown in figure 11(a) and 11(b) respectively. From the figure one can see that there is not much difference between the histograms of both the images. Again a steg-analyst might not see any anomaly in the distribution of the pixel values.

### Table 3. Results of $\chi^2$ attack.

<table>
<thead>
<tr>
<th>Method</th>
<th>C1(%)</th>
<th>C2(%)</th>
<th>C3(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdMod*</td>
<td>61</td>
<td>23</td>
<td>16</td>
</tr>
<tr>
<td>ConDith*</td>
<td>96</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>New Method</td>
<td>90</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

* = These are results taken from [6].
E. Selection of cut-off frequency vs. visual perceptions

Many studies have been done to understand the Human Visual System (HVS). Psychovisual studies have shown that HVS has a general band-pass characteristic. One of the HVS model proposed in [8] describes human sensitivity to spatial frequencies. The model of Contrast Sensitive Function (CSF) for grayscale images is given as:

\[ H(f) = 2.6(0.192 + 0.114f) e^{-0.114f} \]

where \( f = \left( f_x^2 + f_y^2 \right)^{0.5} \) is the spatial frequency in cycles/degree of visual angle. The CSF curve is shown in Figure 13, which indicates that HVS is more sensitive to frequencies around 0.025 and .125 and less sensitive to low and high frequencies. Low frequencies are not useful for steganographic purpose because they are mainly responsible for the creation of Pair of Values (POV’s) which are statistically exploited by steganalysis algorithms. So, the higher frequencies can be exploited to a larger extent. For the embedding algorithm mentioned above, during experimentation we noticed that cut-off frequencies of 0.25 and above hadn’t shown any visual perceptions. However when frequencies below this value are used, the number of bits used for embedding a given magnitude of a HFSI pixel should be reduced so that the changes are imperceptible. So, from our studies we recommend that a cut-off frequency greater than 0.25 be used.

5. Conclusions

In this paper we present a new method of adaptive steganography with its algorithm and application on a sample image. We briefly reviewed some of the existing adaptive steganographic methods and brought out their shortcomings. We have explained how our approach is superior in terms of being able to control the embedding rate using a filtering cutoff frequency \( \theta \). Through extensive experimentation we have shown the higher embedding capacity of this approach. The approach is generic and our method paves a path for new class of steganographic methods which uses both global and local features of an image. Further we have analyzed and compared the proposed approach in terms of the features of choice of embedding capacity, overall higher embedding capacity and resistance to steganalysis. We have seen that in terms of the tests of LSB planes visualization, \( \chi^2 \) attack and histogram analysis our approach has performed in a superior fashion. In the future we propose to give greater analytical details of the largely experimental studies reported here.

Commercial applications of steganography include digital watermarks and digital fingerprinting, which are used to track the copyright and ownership of electronic media. We hope to apply our approach to make digital watermarks so that digital image contents could be made more secure to attacks.

References


Figure 12. Variation of Cut-off frequency vs percentage of message decoded correctly. Original cut-off frequency used at the transmitter is 0.351.

Figure 13: Contrast Sensitive Function [11]


Author Biographies

Atul Negi was born at Bhopal, Madhya Pradesh, India in 1965. He earned his Bachelor of Engineering with Distinction in electronic and communication engineering from the Osmania University, Hyderabad in 1986. He completed his M.Sc.(Eng.) from the Indian Institute of Science, Bangalore India, at their Department of Computer Science and Automation in 1990. He took the Ph.D from the Department of Computer and Information Sciences, University of Hyderabad, Hyderabad India in 1999.

Dr. Negi is a senior member of IEEE, member of the Indian Unit of IAPR. His present research interests include designing optical character recognition systems for Indic scripts. He has served as a referee and on the technical program committees of various national and international conferences. He is also a referee for some international journals. He has chaired sessions for several international conferences and guided more than 50 graduate level dissertations.

Nuthanaganti Santosh Arjun was born at Hyderabad, Andhra Pradesh, India in 1985. He earned his diploma in Electronics and Communication Engineering with Distinction from the Government Polytechnic, Masabtikan, Hyderabad in 2003. He completed his Bachelor of Engineering in Electronics and Communication Engineering from the Osmania University, Hyderabad in 2007.

Mr. Santosh Arjun is an IEEE Student member and ACM Student member. He had five IEEE publications so far. His present research interests include developing steganographic algorithms with high embedding capacity. He chaired the session SC3 at IEEE TENCON 2006 held at Hong Kong.