# A Watermark for Image Authentication using Mapping Code Book

N.Leelavathy
Professor & HOD
Department of CSE
Pragati Engineering College,
Surampalem, India

B.S.Priyatham
Assistant Professor
Department of ECE
UCEK, JNTUK, Kakinada
India

S.Srinivas Kumar
Professor & Director ( R & D)
Department of ECE
UCEK, JNTUK, Kakinada
India

## ABSTRACT

In 2011, Chan proposed a blind image authentication technique by generating the Parity-Check-Bits using Hamming code from a set of pixels whose bits have been reorganized. The Parity-Check-Bits generated are added by modifying other pixels. Due to this rearrangement, the most-significant bit of each suspected pixel can be determined. Using this information, the pixel can be recovered by calculating the average value and selecting one of the two possible original code words. However, calculating the average value, selects the same code word every time yielding to incorrect predictions. Moreover, use of Modulus function to facilitate improvement in quality of embedded image may alter the unused fifth position of each pixel. It is obvious that, the additional one bit or redundancy to detect the correct value may degrade the quality of the authenticated image. This paper proposes the mapping code book to generate Parity-Check-Bits and modified the embedding and recovery algorithms to avoid incorrect predictions and safeguard the fifth position of each pixel. The experimental results prove that the proposed algorithm has a greater capability to recover tampered regions with sufficiently good quality.

## General Terms

Image processing, Security, Authentication, Watermark.

## Keywords

Authentication; Parity-Check-Bits; Tampered; Block effect; Least Significant Bits (LSB); Most Significant Bits (MSB).

## 1. INTRODUCTION

Misappropriations of digital media made seeing is no longer believing. Digital revolution has witnessed drastic advancements in multimedia technology. Images have spread everywhere in no time through various channels such as internet and wireless networks. On one end, sophisticated pixel cameras, scanners, and mobile phones equipped with cameras made it widely available and brought images to common man. Meanwhile, photo-editing software packages and sophisticated computers have helped in extending easy access to manipulate and tamper the digital information on its counterpart. As a consequence, activities like hacking, privacy, forging, and illegal tampering of digital images have taken a lead role, questioning the integrity and security of digital images. As a need in sustaining the existence of digital technology, image authentication techniques have aroused providing security and copyright protecting mechanisms to the vendor. Therefore, image authentication proved to be an important aspect ensuring trust in sensitive application areas like government finance and healthcare.

Image authentication is a process of verifying the authenticity, and integrity of an image. Authentication techniques are

required in order to control the incursion in misusing digital technology. They are usually designed based on two kinds of approaches: data hiding approach or data encrypting approach. Watermarking (fragile, semi-fragile or robust) is a common tool used for hiding the digital information. In contrast, cryptography and digital signatures are employed for encrypting the information. The design of the authentication scheme depends on the strictness of the application. Strict authentication schemes do not tolerate any changes to the host data, but selective considers preserving changes to the image. Both watermarking and cryptographic approaches provide strict and selective authentication schemes. Fragile watermarking and conventional cryptographic methods obey strict authenticating system whereas, semi-fragile and signature methods follow selective authenticating system. These techniques can further be implemented on two domains: spatial and transform. Spatial techniques show simplicity and ease in implementing various techniques. Least Significant Bits (LSB) replacement is usually practiced in spatial techniques. Aside simplicity, it proves to be weak in restraining from affects that commonly occur in the process of communicating over the channels. Transform techniques are robust to affects and perform authentication by using techniques like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), contourlet transform, and wavelet transform, etc.

This paper delivers a new method for image authentication on spatial domain fragile watermarking approach using LSB replacement technique. Mapping code book, which is a grouping combination of the four MSB's on basis of their distance is pioneered as a key concept in implementing the authentication method.

The paper reviews [1] in Section 2. The algorithm proposed in this paper is presented in Section 3. The experimental results are found to exhibit the effectiveness of the proposed method in Section 4. Finally, the conclusions are drawn in Section 5.

## 2. RELATED WORK

In this section, Chan's work [1] is reviewed. Chan's method contains three modules: the embedding, the detection, and the recovery module. The embedding module algorithm generates Parity-Check-Bits [2-4] from the reorganized bits of the pixel and are embed into another pixel, by using modulus function [5]. In the detection module algorithm, the extracted Parity-Check-Bits are recalculated and are used to detect whether the pixel has been tampered or not. According to the indication of the tampered pixels, the tampered areas are detected in the image. In the final phase of the recovery procedure, it recovers the tampered areas after using some morphological operations. The details of Chan's method are described in the following section.

## 2.1 Embedding Algorithm

The embedding algorithm has three steps: Initially, Hamming code is produced, then bits are rotated, and finally, Torus first step, the Automorphism is performed. In the Hamming code production, the Parity-Check-Bits are generated from the rearrangement of four MSBs of each pixel [6]. The relation between generated bits and Parity-Check-Bits is shown in Figure 1.

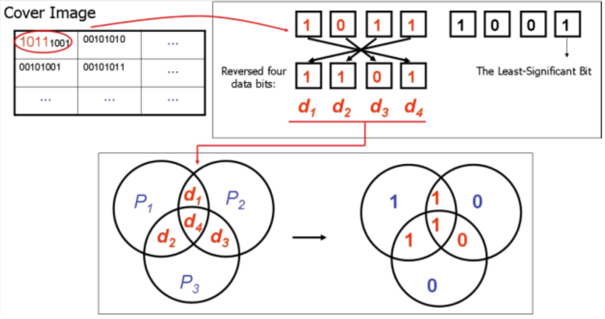


**Fig 1: Generation of the Parity-Check-Bits from reversed bits of pixel.**

The Parity-Check-Bits (P1, P2, P3) can be chosen by considering even number of "1" in each circle. According to the example shown in Figure 1, the Parity-Check-Bits (P1, P2, P3) are 1, 0, and 0, respectively. It should be noticed that the Parity-Check-Bits are generated by first reversing the four MSBs. It is obvious that the Parity-Check-Bits are matched for same MSB of original data bits. Figure 2 shows that, whether the value of the original data bits is more than 128 or not. This can be decided according the value of the Parity-Check-Bits. In the second step, the generated Parity-Check-Bits are rotated to improve security. One secret key, k1 is chosen as a starting point to generate a sequence of random numbers, $R_1, R_2, R_3, \ldots\ldots, R_{N\times N}$, where N is the pixel number of the height and width of the cover image. The random number $R_i$ is selected to rotate $ith$ pixel according to the equation (1).

$$\boldsymbol{J' = (J + R_i)\ mod\ 3} \qquad (1)$$

where $J$ represents the original Parity-Check-Bits, and $J'$ denotes the new rotated Parity-Check-Bits. The variables $J$ and $J'$are both in the range from 0 to 2. The bit at the $J$th position will be rotated to the $J'$th position.

In the third step, the rotated Parity-Check-Bits are embedded into the three least-significant bits of another pixel which is given by the Torus automorphism. The formula of the Torus automorphism is shown as follows.

$$\begin{bmatrix} X_i' \\ Y_i' \end{bmatrix} = \begin{bmatrix} \mathbf{1} & \mathbf{1} \\ \boldsymbol{K_2} & \boldsymbol{K_2+1} \end{bmatrix} \begin{bmatrix} \boldsymbol{X_i} \\ \boldsymbol{Y_i} \end{bmatrix} \boldsymbol{mod\ 3} \qquad (2)$$

where the variable $k2$ represents the second secret key and the $(X_i,\ Y_i)$ denotes the location of the $i$th pixel, $Pi$. On the other hand, the position $(X_i',\ Y_i')$ represents the novel position in which the Parity-Check-Bits of $Pi$ are to be embedded. Once the embedded position for each $Pi$ is known, the Parity-Check-Bits can be embedded by using a modulus function.

In [7], the author has proposed an image hiding scheme using the modulus function. The scheme helps in reducing the variance between the pixel values of the cover image and the embedded image. The scheme modifies the bits other than embedded LSB's to bring the value nearer to the cover pixel.

| Original Data Bits | Reversed Data Bits | Parity Check Bits | The Decimal Values | Distance Between Two Original Data Bits |
|---|---|---|---|---|
| 0 0 0 0 | 0 0 0 0 | 0 0 0 | $(0)_{10}$ | \| 0 - 7 \|= 7 |
| 0 1 1 1 | 1 1 1 0 | 0 0 0 | $(0)_{10}$ | |
| 1 1 1 0 | 0 1 1 1 | 0 0 1 | $(1)_{10}$ | \| 14 - 9 \|= 5 |
| 1 0 0 1 | 1 0 0 1 | 0 0 1 | $(1)_{10}$ | |
| 1 0 1 0 | 0 1 0 1 | 0 1 0 | $(2)_{10}$ | \| 10 - 13 \|= 3 |
| 1 1 0 1 | 1 0 1 1 | 0 1 0 | $(2)_{10}$ | |
| 0 1 0 0 | 0 0 1 0 | 0 1 1 | $(3)_{10}$ | \| 4 - 3 \|= 1 |
| 0 0 1 1 | 1 1 0 0 | 0 1 1 | $(3)_{10}$ | |
| 1 1 0 0 | 0 0 1 1 | 1 0 0 | $(4)_{10}$ | \| 12 - 11 \|= 1 |
| 1 0 1 1 | 1 1 0 1 | 1 0 0 | $(4)_{10}$ | |
| 0 0 1 0 | 0 1 0 0 | 1 0 1 | $(5)_{10}$ | \| 2 - 5 \|= 3 |
| 0 1 0 1 | 1 0 1 0 | 1 0 1 | $(5)_{10}$ | |
| 0 1 1 0 | 0 1 1 0 | 1 1 0 | $(6)_{10}$ | \| 6 - 1 \|= 5 |
| 0 0 0 1 | 1 0 0 0 | 1 1 0 | $(6)_{10}$ | |
| 1 0 0 0 | 0 0 0 1 | 1 1 1 | $(7)_{10}$ | \| 8 - 15 \|= 7 |
| 1 1 1 1 | 1 1 1 1 | 1 1 1 | $(7)_{10}$ | |

**Fig 2: Original data bits and the Parity-Check-Bits.**

A secret value $s$ is assumed with $k$ - bit length which is to be embedded in the cover pixel with value $y$. The motive of Thien's hiding scheme is to modify the gray scale pixel $y$ to $y'$ such that $y'$ is the nearest value to the original pixel $y$ among all possible set of values but also satisfies the condition that

$$\boldsymbol{y'\ mod\ 2^k = s} \qquad (3)$$

To accomplish this, the difference value $d$ is computed by

$$\boldsymbol{d = s - (y\ mod\ 2^k)} \qquad (4)$$

The d value is then further modified to reduce its value as-

$$\mathbf{d'} = \begin{cases} \mathbf{d} \quad \mathbf{if} \left(-\left[\frac{\mathbf{2^k-1}}{\mathbf{2}}\right]\right) \le \mathbf{d} \le \left(\left[\frac{\mathbf{2^k-1}}{\mathbf{2}}\right]\right), \\ \mathbf{d + 2^k} \quad \mathbf{if} \left(-\mathbf{2^k+1}\right) \le \mathbf{d} \le \left(-\left[\frac{\mathbf{2^k+1}}{\mathbf{2}}\right]\right), \\ \mathbf{d - 2^k} \quad \mathbf{if} \quad \left(\left[\frac{\mathbf{2^k-1}}{\mathbf{2}}\right]\right) < d < \mathbf{2^{k.}} \end{cases} \qquad (5)$$

Finally, the modified value $y'$ can be obtained by adding the tailored difference value $d'$ to the original grayscale pixel $y$.

$$\mathbf{y' = d' + y} \qquad (6)$$

## 2.2 Detection and Recovery Algorithm

The importance of the detection algorithm is to trace the tampered areas so that the recovery procedure has target areas to recover. In the detection algorithm, the Parity-Check-Bits of the pixel $Pi$ at ($xi$, $yi$) are extracted from the pixel at ($xi$,$yi$) according to (2). Simultaneously, the Parity-Check-Bits of the pixel $Pi$ are found out through the four most-significant bits of the pixel $Pi$. Once the extracted Parity-Check-Bits are not identical to the produced bits, both the positions ($xi$, $yi$) and ($xi$, $yi$) are marked as tampered pixels. After checking all pixels, morphological operations are performed to eliminate the isolated faulty marked tampered pixels. Finally, the tampered areas are located through the detection algorithm.

In the recovery algorithm, if the Parity-Check-Bits of the tampered pixel are not modified, these bits can be used to predict the value of the tampered pixel. According to the value of the Parity-Check-Bits, the value of the most significant bit, $d4$, can be predicted. According to Figure 2, the value of the MSB of the pixel can help us to select the correct one out of two candidates so as to recover the tampered pixel. More precisely, in the detection procedure, the tampered area has been located. Chan's method uses an indicated matrix **M** to indicate the number of the surrounding untampered pixels for each tampered pixels.

The tampered pixels with a larger pixel value at the positions indicated by matrix **M** have a better chance to select a correct one from two candidates because they have the opportunity of having more untampered pixels as references. Hence, only the pixels values having the largest number of untampered pixels will be processed in each round. As the MSB of the predicted pixel can be known by referring to the Parity-Check-Bits, the untampered pixels whose MSB is the same as the predicted pixel are gathered to calculate their average value. The candidate that has the minimal distance with the average value is selected to recover this tampered pixel. After that, the recovered pixels are marked as untampered pixels, and the same procedure is repeatedly performed to recover tampered pixels until all tampered pixels are made as untampered pixels. The recovery procedure is shown in Figure 3.

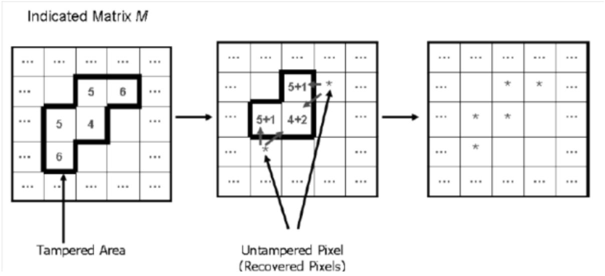


**Fig 3: Recovery Procedure**

# 3. PROPOSED METHOD

In Chan's method, the Parity-Check-Bits are used to find the value of the MSB. But, the method has to predict pixels correctly by selecting one from two candidates. The prediction scheme faces severe challenges in selecting one from the two candidates by using averaging method described in section 2.2. The selection that is based on the average values of the most significant pixels and the difference of the original bits are always constant. Hence the scheme selects only one possibility every time even though the other is the original combination of bits. But still, Chan's method works good because, the distance between the two original bits of a set are ‘1’, ‘3’ , ‘5’ and ‘7’, where only the distance of ‘7’ can only be noticed through human eye. Furthermore, use of Thien's hiding scheme may tamper the fifth unused bit in order of reducing the embedding variance of the three least significant bits. Tampering the unused fifth bit alters the value of eight gray scale levels in the process of reducing the embedding variance.

Thus, to encounter the problems and issues aroused in the Chan's method the proposed scheme adopted Mapping code book with a constant variance of eight between the two original bits. This gave the flexibility in selecting the exact original bits with high constant distance. Further, averaging of local pixels surrounding the tampered pixel is preferred against Chan's method. The embedding and retrieval procedures of both Chan's method and the proposed technique seems to be same as discussed in section 2, but changes are made at some instances to yield better results. In the embedding algorithm, the proposed method is almost similar as Chan's method except for the Hamming code production step.

Chan's method obtained authentication data from four MSB by producing Parity-Check-Bits. On contrary, our proposed method obtains authentication data from four MSB through the Mapping Codebook as shown in Figure 4. The mapping value can be decided by referring to the four MSB and the Mapping Codebook.

| Original Data Bits | The Decimal Values | Absolute Difference between Original Bits | Embedding Bits |
|---|---|---|---|
| 0 0 0 0<br>1 0 0 0 | $(0)_{10}$<br>$(-8)_{10}$ | 8 | 0 0 0 |
| 0 0 0 1<br>1 0 0 1 | $(-1)_{10}$<br>$(-9)_{10}$ | 8 | 0 0 1 |
| 0 0 1 0<br>1 0 1 0 | $(-2)_{10}$<br>$(-10)_{10}$ | 8 | 0 1 0 |
| 0 0 1 1<br>1 0 1 1 | $(-3)_{10}$<br>$(-11)_{10}$ | 8 | 0 1 1 |
| 0 1 0 0<br>1 1 0 0 | $(-4)_{10}$<br>$(-12)_{10}$ | 8 | 1 0 0 |
| 0 1 0 1<br>1 1 0 1 | $(-5)_{10}$<br>$(-13)_{10}$ | 8 | 1 0 1 |
| 0 1 1 0<br>1 1 1 0 | $(-6)_{10}$<br>$(-14)_{10}$ | 8 | 1 1 0 |
| 0 1 1 1<br>1 1 1 1 | $(-7)_{10}$<br>$(-15)_{10}$ | 8 | 1 1 1 |

**Fig 4: Mapping Code Book**

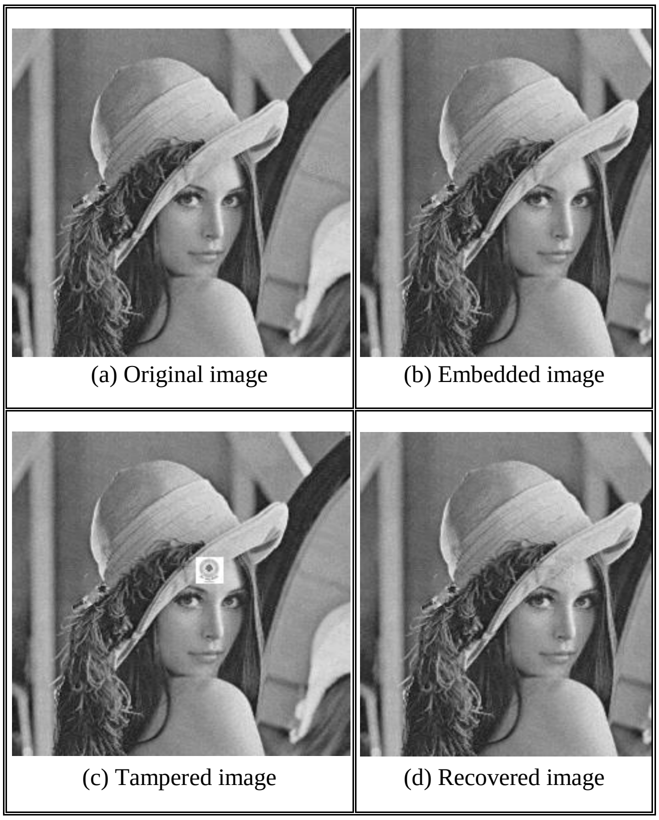
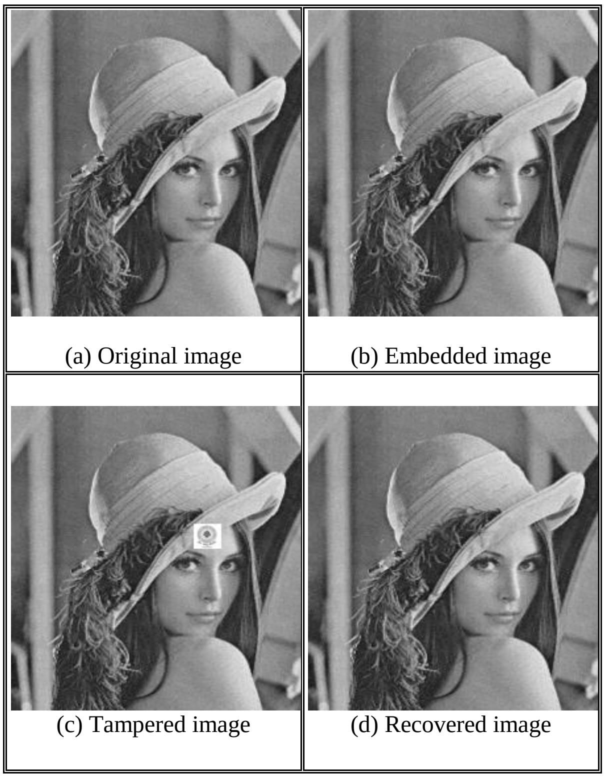

(a) Original image
(b) Embedded image
(c) Tampered image
(d) Recovered image

**Fig 5: Results for Chan's method (PSNR: 35.82915)**

The role of the mapping value is treated as the parity bits in Chan's method. The mapping value has to perform the steps of bit rotation. The rotated bits are embedded to the three least-significant bits of another pixel indicated by Torus Automorphism. Simultaneously, with the process of embedding the information is put into the LSB of the selected pixel, and fifth bit is indicated in a separate dummy matrix of same dimension of the image.

After applying the Thien's hiding scheme to the image all the fifth bit of the corresponding pixels are replaced into their corresponding positions. Furthermore, the number of unaltered bits ‘N’ in Thien's hiding scheme is increase to ‘4’ from ‘3’ in the process of protecting the fifth bit from tampering. In the recovery process, to recover the tampered pixel, local pixel averaging is preferred. The highest number of untampered pixels surrounding the tampered pixel is selected and the average value of all the untampered pixels is replaced in the tampered pixel as a recovered value.


(a) Original image

(b) Embedded image

(c) Tampered image

(d) Recovered image

**Fig 6: Results for proposed method (PSNR:51.30392)**

## 4. EXPERIMENTAL RESULTS

Experimentation is done with a standard Lena test image of dimensions 512 × 512. The proposed method showed better results compared to the Chan's method. Block effect due to incorrect predictions has totally been eliminated. The new scheme improved the signal to noise ratio. The recovered images of both Chan's and the proposed along with PSNR values are given in the Figure 5 and Figure 6.

Table 1 and Table 2 shows the experimental performance of tampering on different areas of the Lena image and tampering on different images respectively in terms of PSNR.

## 5. CONCLUSIONS

In this paper, we group four most-significant bits into different groups to form a mapping codebook. The mapping codebook is used to replace the role of (7, 4) Hamming code book in Chan's method. The mapping codebook has two important properties. Firstly, only the candidates with the same value of the most significant bit can be gathered in the same group. This means that the value of the MSB of the predicted pixel can be decided according to its mapping values. Finally, the distance between two candidates of each group is constant, so that incorrect predictions can be avoided. Mapping code book of distance eight have given maximum flexibility in predicting the original bits and use of averaging, based on the surrounding pixels, have strengthen the recovery in reducing the number of incorrect predictions. Double Torus automorphism usage in the embedding phase has increased the complexity of the embedding scheme, but showed drastic changes in the quality of the embedded image due to fifth bit conservation. Finally, the quality measure like PSNR has obeyed to the efficiency of the method and has given positive results in all directions. Experimental results have proved better signal to noise ratio and the quality of the recovered image is better than the previous method.

## 6. FUTURE SCOPE

In implementing a profound technique, with a detailed study and considerations on the issues pertained in the existing technique, several new ideologies have shown its face. Being aware of the importance of authentication schemes in modern world, the ideologies have better scope to implement and apply of various applications. Starting with the concept of image, authentication schemes can further be developed on videos, considering individual video frames. This technique can also be implemented for color images preferring ‘R’ ‘G’ ‘B’ planes.

Authentication schemes may also be implemented as an application for intra departments of image processing. This technique has ample scope in the fields of finger printing, ear identification and several other areas where accessing is given prime importance.

## 7. REFERENCES

[1] Chan, C. S. An image authentication method by applying Hamming code on rearranged bits. *Pattern Recognition Letters*, 2011, *32*(14), 1679-1690.

[2] Chan, C. S., & Chang, C. C. An efficient image authentication method based on Hamming code. *Pattern Recognition*, 2007, *40*(2), 681-690.

[3] Hamming, R. W. Error detecting and error correcting codes. *Bell System technical journal*, 1950, *29*(2), 147-160.

[4] Dadkhah, S., Manaf, A. A., & Sadeghi, S. Efficient Two Level Image Tamper Detection Using Three LSB Watermarking. *Fourth International Conference on Computational Intelligence and Communication Networks (CICN)*, IEEE Nov., 2012.

[5] Chan, C. S., Lin, C. Y., & Lin, Y. H. Apply the modulus function to secret image sharing. *International Journal of Innovative Computing Information And Control*, *8*(1 A), 2012, 375-385.

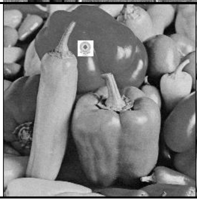
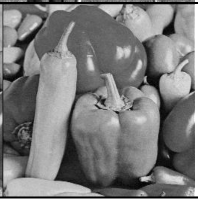
[6] Chan, C. S., Tsai, Y. Y., & Liu, C. L. An Image Authentication Method by Grouping Most Significant Bits, Journal of Electronic Science and Technology, Vol. 11, March 2013.

[7] Thien, C. C., & Lin, J. C. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. *Pattern Recognition*, *36*(12), 2875-2881, 2003.

**Table 1. Performance of tampering on different areas of the Lena image**

| Lena | Embedded Image | Detected Image | Recovered Image | PSNR Value |
|---|---|---|---|---|
| **Hat** | | | | **53.18** |
| **Hair** | | | | **53.96** |
| **Face** | | | | **51.30** |
| **Back ground** | | | | **53.30** |

**Table 2. Performance of tampering on different images**

| Images | Embedded Image | Detected Image | Recovered Image | PSNR Value |
|---|---|---|---|---|
| **Lena** | | | | **53.179139** |
| **Barbara** | | | | **51.401803** |
| **Camera-man** | | | | **44.215774** |
| **Peppers** | |  |  | **44.514125** |