Data Embedding using Secured Adaptive Pixel Pair Matching

Mr. Swapnil S. Thakare¹, Prof. Niranjan L. Bhale²

¹PG Student, Department of Computer Engineering, Matoshri College of Engineering and Research Center, Nashik, Pune University, MS, India

²Department of Information Technology, Matoshri College of Engineering and Research Center, Nashik, Pune University, MS, India

Abstract
Steganography can be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. Steganography is now more important due to need of secure communication in this era of potential and vulnerable computer users. The essential idea of Secured APPM is to use the values of pixel pair as a reference coordinate and search or finds that coordinate within the newly and specially designed compact neighborhood set of this pixel pair according to a given message digit. Then that pixel pair is gets replaced by the searched coordinate to hide / conceal the digit. It also provide adjustable payload and allows users to select digits in any notational system for data embedding, and thus achieves a better image quality. As Secured APPM does not produce any artifacts in stego images the steganalysis results are similar to those of the cover images so it offers a secure communication under adjustable embedding capacity. It also contains additional features such as digital watermark and encryption of secret messages for the provision of more security. The secured APPM technique is also able to hide all different types of data provided to it in languages like English, Marathi, Hindi etc. Secured APPM has become straightforward, economical embedding method for the data hiding by removing the various shortcomings found in the various previous techniques based on PPM, such as low-payload problem in EMD. It also offers smaller MSE than the OPAP, DE and APPM. As well as this technique is secure under the detection of some well-known steganalysis techniques.

Keywords:- Steganography, Adaptive Pixel Pair Matching (APPM), Diamond Encoding (DE), Exploiting Modification Direction (EMD), Least Significant Bit (LSB), Optimal Pixel Adjustment Process (OPAP), Encryption, Digital Watermark.

1. INTRODUCTION
As need of Internet-based applications is highly increased, so it is required to use the secrecy in communication. To achieve this goal, there are mainly three techniques are available, cryptography, watermarking and steganography. Steganography is the art of hiding information through original object/carrier in such a manner that the existence of the message is unknown. The term steganography is comes from Greek word Steganos, which means, “Covered Writing”. The original objects can be referred to as covered/carrier objects. After inserting the secret message in to the cover image it is called as stego image. A stego key is used for hiding. [4][5][6][7] Steganography is different from cryptography. The main objective of cryptography is to secure communications by using encryption techniques. But steganography techniques are used to hide the messages, which makes difficult for a third party / person to find out the message. [4] Watermarking and fingerprinting related to steganography are basically used for intellectual property protection. [4][5][6][7].

2. DIFFERENT KINDS OF STEGANOGRAPHY
The five main categories of file formats that can be used for steganography are:

2.1 Text Steganography
This method is used to hide a secret message in a text message for that number of tabs, white spaces, and capital letters, just like Morse code is used. In earlier day this technique is in very much boom but after booming of Internet and different type of digital file formats its importance gets decreased. [4][5][6][7]

2.2 Image Steganography
Digital images are widely used over the internet as well as that are also popular. Now using this phenomenon the digital images can be used as a cover images/objects for the steganography. In this technique a secret message is embedded/hide in a digital image through an embedding procedure/algorithm with the help of secret key to produce a stego image. [4][5][6][7]

2.3 Audio Steganography
Audio stenography is another type of steganography in which the properties of the human ear is considered to hide information. An audible, sound can be made inaudible in the presence of another louder audible sound. Audio steganography uses only digital audio formats such as WAVE, MIDI, AVI MPEG or etc. [4][5][6][7]

2.4 Video Steganography
Video Steganography is a technique used to hide any kind of files or information into digital video format. Here video is used as carrier for hidden information. Video steganography uses following types of video files such as
H.264, Mp4, MPEG, AVI or other video formats.

2.5 Protocol Steganography

The term protocol steganography is to embedding information within network protocols such as TCP/IP. We can hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used. The protocol steganography uses the TCP, UDP, IP network protocols for data hiding. [4][5][6][7]

3. STEGANOGRAPHIC TECHNIQUES

Digital image steganography techniques can be divided into following domains:

2.6 Spatial Domain Techniques

There are many versions present in spatial steganography that all are related to make changes directly with some bits of the digital image pixel values to hide data. [4][5][6][7]

Least significant bit (LSB) - based steganography is one of the simplest techniques/method that is used to hide a secret message in digital image. In this technique the pixel value of least significant bit (LSB) are get replaced with bits of secret message and all this is done without introducing many perceptible distortions. The embedding of message bits can be done either sequentially or randomly. [4][5][6][7] In spatial domain following techniques comes these are as follows such as LSB substitution/replacement, LSB matching, Matrix embedding and Pixel value, differencing etc. [4] [5] [6] [7]

2.7 Transform Domain Techniques

This is a more complex technique of hiding information in an image. In this various transformation algorithms are used to hide data behind the image [4]. This technique also is termed as a domain of embedding techniques. In this technique a number of algorithms are exists. Most of the strong steganographic systems work in the transform domain because the process of embedding data in the frequency domain of a signal is much stronger than any other domain such as time or etc. [4][5][6][7] Transform domain techniques are more advantageous than spatial domain because it hides information in such parts of image that are less exposed to image processing, cropping and compression.

Transform domain techniques are mainly classified as follows:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT).
5. Embedding in coefficient bits

2.8 Distortion Techniques

This technique works on the principle of differences between the cover image and the stego image and for that it needs to keep a track of cover image. While embedding the secret message by this technique the encoder adds a sequence of changes to the cover image i.e. way in which and how/where the secret message get embedded. For this process the difference in the signal distortion is considered. [4][5][6][7] But before the embedding a secret message into the cover image it has to encode it for that the encoder chooses the pixels of cover image pseudo-randomly and changes that pixel bit with message bit in a such manner the statistical properties of the image are not get affected. [4][5][6][7] However, this method has one drawback as cover image should never be used more than once. As well as an attacker can easily tampers the stego-image by cropping, scaling or rotating. [4][5][6][7]

2.7 Masking and filtering

This technique has resemblance with the technique of paper watermark. In this technique information is get concealed by marking an image for that purpose it uses the noise levels of the cover images. The main advantage of this technique is that the hidden message is more integral to the cover image and watermarking techniques can be easily applied as well as there is no fear of image destruction. [4][5][6][7] This method has one more advantage as it is much more robust than LSB replacement with respect to comparison made based on the following the categories such as compression and the information is hidden in the visible parts of the image. [4][5][6][7] This technique also has the disadvantage as it only works on gray scale images. [4][5][6][7]
3. LITERATURE SURVEY

This section provides the knowledge of different data hiding techniques are used to hide the data. These are as follows:

3.1 Pixel Value Differencing (PVD)

In Paper “An Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods” author proposed a Pixel value difference (PVD) and simple least significant bits scheme are used to achieve adaptive least significant bits data embedding. In pixel value differencing (PVD) where the size of the hidden data bits can be anticipated by difference between the two consecutive pixels in cover image using simple relationship between two pixels. PVD method provides a better imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. [8] This method hides large data with the help of LSB substitution at edge area of image and uses the PVD for smooth region of image to hide the data. Though this technique provides larger capacity but has low visual quality as well as this method is complex. [4][5][6][7][8]

3.2 LSB Substitution

In paper “Hiding Data in Images by Simple LSB Substitution” authors proposed an LSB substitution for hiding the data into the image. To achieve better visual quality of stego-image it takes care of noise sensitive area for embedding. This method intelligently differentiates normal texture and edges area of an image as well as it takes the advantage of these areas for the embedding. This method analyses the different LSB values as well as edges, texture masking and brightness of the cover image to calculate the number of k-bit LSB for secret data embedding. It also utilizes the pixel adjustment method for better stego-image visual quality through LSB substitution method. [4][5][6][7][10] Optimal pixel adjustment process is also used to generate the stego-image which is obtained by the simple LSB substitution method. The proposed method also termed as OPAP (Optimal Pixel Adjustment Process). [10] The overall result shows a good high hidden capacity with high image quality of the stego-image can be greatly improved with low extra computational complexity. [10] The main shortcoming of this technique is the worst mean-square-error between the stego-image and the cover-image is derived. [4][5][6][7][10]

3.2.1 Mathematical Model of LSB Substitution

Let Z be the original cover-image of M × N pixels represented as:

\[ Z = X_{ij} 0 \leq i \leq M, 0 \leq j \leq N, \]
\[ X_{ij} \in \{0,1,2, \ldots, 255\} \]

\( M \) be the n-bit secret message represented as

\[ T = \{t_i | 0 \leq i \leq n, t \in \{0,1\} \} \]

Suppose that the n-bit secret message \( T \) is to be embedded into the \( k \)-rightmost LSBs of the cover-image \( Z \). Firstly, the secret message \( T \) is rearranged to form a conceptually \( k \)-bit virtual image \( T' \) represented as [10]

\[ T' = \{ t'_i | 0 \leq i \leq n', t_i \in \{0,1, \ldots, 2^{k} - 1\} \} \]

Where \( n' < M \times N \); the mapping between the \( k \)-bit secret message \( T = \{t_i\} \) and the embedded message \( M' = \{m_i'\} \) can be defined as follows: [10]

\[ t'_i = \sum_{j=0}^{k-1} t_{i \times j} \times 2^{k-1-j} \]

A subset of \( n' \) pixels \( \{x_1', x_2', \ldots, x_n'\} \) are chosen from the cover-image \( Z \) in a predefined sequence. The embedding process is completed by replacing the \( k \) LSBs of \( xi \) by \( ti' \). Mathematically, the pixel value \( x'i \) of the chosen pixel for storing the \( k \)-bit message \( ti' \) is modified to form the stego-pixel \( x'i \) as follows: [10]

\[ x'_i = x'_i - x'_i \mod 2^k + t_i \]

In the extraction process, given the stego-image \( S \), the embedded messages can be readily extracted without referring to the original cover-image. [10] Using the same sequence as in the embedding process, the set of pixels \( \{x'_1, x'_2, \ldots, x'_n\} \) storing the secret message bits are selected from the stego-image. The \( k \) LSBs of the selected pixels are extracted and lined up to reconstruct the secret message bits. Mathematically, the embedded message bits \( ti' \) can be recovered by [10]

\[ t'_i = x'_i \mod 2^k \]

3.3 Exploiting Modification Direction (EMD)

In paper “Efficient Steganographic Embedding by Exploiting Modification Direction” author provides a new approach to data hiding scheme by introducing a novel method of steganographic embedding in digital images is described, in which each secret digit in a \( 2(n+1) \) notational system is carried and hide by \( n \) pixels of the cover image. In this method at most only one pixel is increased or decreased by 1. It is not suitable for applications that requiring high payload is the main shortcoming of this technique. [4][5][6][7][9]

3.4 Diamond Encoding (DE)

In paper “A Novel Image Data Hiding Scheme with Diamond Encoding” author provides a new approach to data hiding scheme by introducing Diamond Encoding. In this technique, first the process is portioning and embedding of the cover image into non-overlapping blocks of two consecutive pixels. Then it transforms the secret messages into a series of digits which are equivalent to those blocks. Afterward the diamond encoding technique is applied on those blocks to calculate the diamond characteristic values i.e. DCV to hide/concealed secret – ary digits into the diamond characteristic values. After that the diamond characteristic value is gets modified by secret message digit and which can be done by adjusting pixel values in blocks. The main shortcoming of this technique is that it suffers from higher distortion for various lower payload with lower image quality and can be attacked by
some well-known steganalysis techniques as well as it does not provide more compact Neighborhood sets. It also not allows embedding digits in any notational system. [4][5][6][7][3]

3.4.1 Mathematical Model of DE

The DE method is briefly described as follows. Let the size of Z bits cover image be $U_x \times U_y$, message digits be $T_B$, where the subscript B represents $T_B$ is in a B-ary notational system. First, the smallest integer $k$ is determined to satisfy the following equation: [3]

$$\left\lfloor \frac{U_x \times U_y}{2} \right\rfloor \geq |T_B|$$

Where $|T_B|$ denotes the number of message digits in a B-ary notational system. To conceal a message digit $T_B$ into pixel pair $(x, y)$ the neighborhood set $\mathcal{O}(x, y)$ is determined by [3]

$$\mathcal{O}(x, y) = \{(a, b) | |a - x| + |b - y| \leq k\}$$

Here $\mathcal{O}(x, y)$ represents the set of the coordinates $(a, b)$ and its absolute distance to the coordinate $(x, y)$ that is smaller or equal to $k$. A diamond function $f$ is then employed to calculate the DCV of $(x, y)$. Where $f(x, y) = \{((2k+1)x + y) \mod B\}$. [3] After that, the coordinates belong to the set $\mathcal{O}(x, y)$ are searched and DE algorithm finds a coordinate $(x, y)$ that satisfy $f(x', y') = T_B$ and then $(x, y)$ is get replaced by $(x', y')$. [3] Repeat these procedures until all the message digits are embedded. In the extraction phase, pixels are scanned using the same order as in the embedding phase. The DCV value of a pixel pair is then extracted as a message digit. [3]

3.5 Adaptive Pixel Pair Matching (APPM)

In paper “A Novel Data Embedding Method Using Adaptive Pixel Pair Matching” author proposed APPM Method in that it first selects the pixel pair then use that pixel pair’s value as reference coordinate. After that it searches the coordinate in the neighborhood set of these pixel pairs according to a given message digit after that the pixel pair is then replaced by the searched coordinate to obscure the digit. It has chance of future improvement in case of high definition color images and further more it is possible to improve it for more high data capacity and with more security. [4][5][6][7][2]

3.6.1 Mathematical model of APPM

The basic idea of the PPM-based data-hiding method is to use pixel pair $(p, q)$ as the coordinate, and searching a coordinate $(p', q')$ within a predefined neighborhood set $\mathcal{O}(p, q)$ such that $f(p', q') = T_B$, where $f$ is the extraction function and $T_B$ is the message digit in a B-ary notational system to be concealed. Data embedding is done by replacing $(p, q)$ with $(p', q')$. [2]

Now suppose consider the cover image $Z$ is of size $U_x \times U_y$ and $T$ is the message bits to be concealed. [2]

$[7]$ is the size of $T$; now first calculate the minimum $B$ such that all the message bits can be embedded. Then, message digits are sequentially concealed into pairs of pixels. But while embedding the message bits in to image firstly check the minimum $B$ satisfying $\left\lfloor \frac{U_x \times U_y}{2} \right\rfloor \geq |T_B|$, and convert $T$ into a list of digits with a B-ary notational system $T_B$. The discrete optimization problem is solved to find $C_a$ and $\mathcal{O}_b(p, q)$. In the region defined by $\mathcal{O}_b(p, q)$, record the coordinate $(p', q')$ such that $f(p', q') = i, 0 \leq i \leq B - 1$. [2] Construct a non-repeating random embedding sequence $Q$ using a key $K_r$. To embed a message digit $T_B$, two pixels $(p, q)$ in the cover image are selected according to the embedding sequence $Q$, and calculate the modulus distance $G = (T_B - f(p, q)) \mod B$ between $T_B$ and $f(p, q)$ then replace $(p, q)$ with $(p + p', q + q')$. [2]

3.6 Other Techniques

In paper “LSB matching revisited” author provides a new approach to data hiding scheme by revisiting the previous LSB substitution method by replacing it with the new approach. Here the author introduced the LSB matching choice, in that it decides whether to add or subtract one from the cover image pixel and it is done purely on random basis. This new method uses the choice set of a binary function to select the at most two cover pixels of the required value. Then the actual embedding is done using a pair of pixels selecting/taken as a unit. Now in this process the LSB of the first pixel carries only one bit of secret message and another one carries another bit of secret message. [11] The main shortcoming of this technique is that it made fewer changes in the original image. [4][5][6][7][11] In Paper “Matrix Embedding for Large Payloads” authors proposed Matrix Embedding method in that common pattern of bits are made by using the combination of P x Q size rows and columns (of a block/matrix) with the help of random key value. In embedding procedure, each and every pattern of bits is matched with secret message bits, if that pattern get matched and satisfied then it modifies the LSB bits of cover image with the secret message bits, otherwise cover image remains the same. This technique is mainly used to achieve to get security of hidden message in stego-image using a common pattern key. This proposed method has low hidden capacity because to hide only single secret bit it requires a block of (P x Q) pixels. [4][5][6][7][12] In paper “A Double Layered “Plus-Minus One” Data Embedding Scheme” author proposed method that uses the pixels to hide a data. First select a pixel now set their grayscale value and then by adding/subtracting one to/from the gray value we can hide data to an image. In this author also used binary covering codes and wet paper codes to hide messages in the LSB plane and the second LSB plane, respectively. [1] Using this method author achieved the upper bound on the embedding efficiency. [1][4][5][6][7]

4. Proposed Secure APPM Methodology

APPM is proved to offer security against detection and lower distortion but it has further chance of improvement so the proposed method will take forward APPM for colored images to explore a better mechanism and lower distortion for embedding data in colored images as well as
grayscale images with better security and more embedding capacity in terms of payload and performance that can be improved. [2] The PPM-based method, suppose a digit $T_B$ is to be concealed. The range of $T_B$ is between 0 and B-1, and a coordinate $(p', q')$ in $\mathcal{O}(p, q)$ has to be found such that $f(p', q') = T_B$. [2] Therefore, the range of $(p, q)$ must be integers between 0 and B-1, and each integer must occur at least once. In addition, to reduce the distortion, the number of coordinates in $\mathcal{O}(p, q)$ should be as small as possible. The best PPM method shall satisfy the following three requirements:

1) There are exactly B coordinates in $\mathcal{O}(p, q)$. [2]
2) The values of extraction function in these coordinates are mutually exclusive. [2]
3) The design of $\mathcal{O}(p, q)$ and $f(p, q)$ should be capable of embedding digits in any notational system so that the best can be selected to achieve lower embedding distortion. [2]

The definitions of $\mathcal{O}(p, q)$ and $f(p, q)$ significantly affect the stego image quality. The designs of $\mathcal{O}(p, q)$ and $f(p, q)$ have to fulfill the following requirements:

- All values have to be mutually exclusive and the summation of the squared distances between all coordinates in $\mathcal{O}(p, q)$ and $f(p, q)$ has to be the smallest. [2]
- This is because, during embedding, $(p, q)$ is replaced by one of the coordinates in $\mathcal{O}(p, q)$. [2]
- Suppose there are B coordinates in $\mathcal{O}(p, q)$, i.e., digits in a B-ary notational system are to be concealed, and the probability of replacing $(p, q)$ by one of the coordinates in $\mathcal{O}(p, q)$ is equivalent. [2]
- The averaged MSE can be obtained by averaging the summation of the squared distance between and other coordinates in $\mathcal{O}(p, q)$. Thus, given a $\mathcal{O}(p, q)$, the expected MSE after embedding can be calculated by

$$MSE_{\mathcal{O}(p,q)} = \frac{1}{2} \sum_{i=0}^{B-1} \{(p_i - p)^2 + (q_i - q)^2\}$$

1) The solution of $\mathcal{O}(p, q)$ and $f(p, q)$ is indeed a discrete optimization problem

$$\minimize: \sum_{i=0}^{B-1} \{(p_i - p)^2 + (q_i - q)^2\}$$

subject to: $f(p_i, q_i) \in \{0, 1, \ldots , B - 1\}$

$$f(p_i, q_i) \neq f(p_j, q_j) \text{ if } i \neq j$$

$$0 \leq i, j \leq B - 1$$

4.2 Embedding Procedure

The embedding module accepts the encrypted secret message as input from encryptor module and process on it to embed that encrypted secret message in to cover image as a steganography for the secret communication. The output of this embedding module is the stego image which contains a secret message. [2] Suppose the cover image is of size $U \times U$ and M is the message bits to be concealed. The size of is $T$ is $[7]$ and key Er. [2]

1) Find the minimum of $B = (2d^2 + 2d + 1)$, $d \geq 1$ satisfying $\left\lfloor \frac{U \times U}{2B} \right\rfloor \geq |T_0|$ and convert T into a list of digits with a W-ary notational system $|T_0|$. [2]
2) Solve the discrete optimization problem to find $C_B$ and $\mathcal{O}(p, q)$. [2]
3) In the region defined by $\mathcal{O}(0, 0)$, record the coordinate $(p_0, q_0)$ such that $T_0, p_0, q_0 = 101\ldots 1$.
4) Construct a non-repeat random embedding sequence j using a key Er. [2]

4.1 Encryption and Decryption Procedure

Before embedding or hiding the secret message in to the cover image it is inputted to encryptor for the encryption. As well as after the extraction process again this secret message is passed to decryptor for decryption and then the original message is obtain. The advantage of this methodology is that it protects the secret message from the attacker under the steganalysis attack. [2] In addition to English language, this secured APPM technique is also able to hide data provided in different languages such as Marathi, Hindi etc. [2]

4.2 Extraction Procedure

The extraction module accepts the stego image which contains secret message as an input from the embedding module. The extraction module process on that input and generate cover image and encrypted secret message. This encrypted secret message is then pass to decryptor module to generate plain secret message. [2] To extract the embedded message digits, pixel pairs are scanned in the
same order as in the embedding procedure. The message digits which were embedded in the previous phase is considered / forwarded as the parameter values of extraction function which is got from the scanned pixel pairs. [2]
1) Construct the embedding sequence j using the key Hr.
2) Select two pixels (p', q') according to the embedding sequence j. [2]
3) Calculate I (p', q') and the result is the embedded digit.
4) Repeat Steps ii and iii until all the message digits are
5) Finally, the message bits T can be obtained by converting the extracted message digits into a binary bit stream. [2]

4.3 Digital Watermark
In digital watermark module a digital watermark is implemented. A digital watermark is a kind of marker which is secretly embedded in a noise-tolerant signal such as image, video, audio and text etc. Digital watermarks may be used to verify the authenticity; integrity of the carrier signal as well as it shows the identity of its creator/owner. It gives a reciprocal reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (Authentication and non repudiation) and that the message was not altered in transit (i.e. to maintain integrity). As well as watermark gives integrity of message. The digital watermark gives authentication for secured communication. In this system message received from sender is in authenticated form and with security in communication. Due to this sender cannot deny about message sent by him and this also assures that message was not altered in transit. [16]

5. THEORETICAL MSE ANALYSIS
Distortion in an image occurs when data are embedded in it, which in turns results in to modification of pixel values of the image and due to this the original quality of image gets changed. The MSE is used to measure the quality of image. [2]

\[
MSE = \frac{1}{UXU} \sum_{i=0}^{U} \sum_{j=0}^{U} (p_{ij} - p'_{ij})^2
\]

Where UXU denotes the image size, p_{ij} and p'_{ij} denote the pixel values of the original image and the stego image, respectively. MSE represents the mean square error between the cover image and stego image. A smaller MSE indicates that the stego image has better image quality. [2]

5.1 Theoretical MSE Analysis for LSB
When data are embedded using LSBs of each pixel, each bit valued 0 or 1 has equal probability. The squared error caused by embedding a bit in the i-th LSB. The averaged MSE is calculated as follows: [10]

\[
MSE_{LSB} = \frac{1}{2} \sum_{i=1}^{r} (2^{i-1})^2 = \frac{1}{6} (4^r - 1)
\]

5.2 Theoretical MSE Analysis for OPAP
Now analyze the average MSE of OPAP when r message bits are embedded in each pixel. Let the original pixel value be v and the stego pixel value be v'. The probability of \(|v - v'| = 0\) or \(2^{r+1}\) is \(1/2^r\) with the probability range of \([1, 2^{r+1} -1]\) is \(1/2^r\). Therefore, the averaged MSE caused by embedding r bits is as follows: [10]

\[
MSE_{OPAP} = \frac{1}{2r} (2^{r-1})^2 + \frac{1}{2r-1} \sum_{i=1}^{2r-1} i^2
\]

\[
= \frac{1}{12} (4^r + 2)
\]

5.3 Theoretical MSE Analysis for DE
For the DE method, consider the probability of selecting coordinate \((x, y)\) in the diamond shaped \(O(x, y)\) to replace a pixel pair \((x, y)\) is the same. Therefore, the averaged MSE caused by embedding digits in a B-ary notational system is as follows and where k is the embedding parameters of DE. [3]

\[
MSE_{DE} = \frac{1}{2B} \sum_{i=0}^{B-1} [(x' - x)^2 + (y' - y)^2]
\]

\[
- \frac{1}{2B} \left[ \sum_{x=0}^{k} \sum_{y=0}^{k} (x^2 + y^2) + \sum_{x=0}^{k} \sum_{y=0}^{k} (x^2 + y^2) \right]
\]

\[
= \frac{k(k+2)(k^2+k+1)}{2+6k(x+y+1)}
\]

5.4 Theoretical MSE Analysis for APPM
For embedding digits in a B-ary notational system using APPM, the probability of replacing \((x, y)\) with \((x', y')\) in \(O(x, y)\) is identical and constant. With the knowledge of \(O(x, y)\), the averaged MSE for grayscale image is obtained by [2]

\[
MSE_{APPM} = \frac{1}{2B} \sum_{i=0}^{B-1} [(x' - x)^2 + (y' - y)^2]
\]

5.5 Theoretical MSE Analysis for Secured APPM
We have apply APPM technique to colour images also with minor improvements in embedding algorithm of APPM which gives slight performance improvement for grayscale and colour images. The averaged MSE is obtained by as follows: [2]

\[
MSE_{secured APPM} = \frac{1}{3B} \sum_{i=0}^{B-1} [(x' - x)^2 + (y' - y)^2]
\]
6. Results and Analysis

This section shows the various types of results of Secured APPM technique with different parameters. These results show improvement over previous APPM techniques with respect to Mean Square Error (MSE). [2] The fig 4 shows the cover and stego images which do not show any artifacts after applying Secured APPM technique to the cover image to hide the secret message in to it. [2]

![Cover Image and Stego Images](image)

Fig. 4. Cover Image and Stego Images
(a) Cover Image (b) Stego Image

![Payload - MSE Relationship Comparison of Various PPM-Based Methods](image)

Fig. 5. Payload - MSE Relationship Comparison of Various PPM-Based Methods

The Table 1 shows the comparison of MSE between the secured APPM technique with the previous technique such as APPM, DE, LSB and OPAP etc.

<table>
<thead>
<tr>
<th>bpp</th>
<th>B</th>
<th>C_B</th>
<th>APPM MSE</th>
<th>Secured APPM MSE</th>
<th>MSE Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>2</td>
<td>0.375</td>
<td>0.25</td>
<td>0.125</td>
</tr>
<tr>
<td>1.161</td>
<td>5</td>
<td>2</td>
<td>0.4</td>
<td>0.1666666</td>
<td>0.23333</td>
</tr>
<tr>
<td>1.850</td>
<td>13</td>
<td>5</td>
<td>1.077</td>
<td>1.0660000</td>
<td>0.011</td>
</tr>
<tr>
<td>2.679</td>
<td>41</td>
<td>6</td>
<td>3.341</td>
<td>3.1666666</td>
<td>0.17433</td>
</tr>
<tr>
<td>3</td>
<td>64</td>
<td>14</td>
<td>5.203</td>
<td>4.8095238</td>
<td>0.39347</td>
</tr>
<tr>
<td>3.205</td>
<td>85</td>
<td>10</td>
<td>6.847</td>
<td>6.8333333</td>
<td>0.01366</td>
</tr>
<tr>
<td>3.410</td>
<td>113</td>
<td>31</td>
<td>9.071</td>
<td>8.6021505</td>
<td>0.46884</td>
</tr>
<tr>
<td>4</td>
<td>256</td>
<td>92</td>
<td>20.518</td>
<td>19.550724</td>
<td>0.96727</td>
</tr>
</tbody>
</table>

The Table 1 shows the improvement of Mean Square Error (MSE) as compared to previous APPM data hiding technique.

**Table 2 MSE Comparison for various types of images**

<table>
<thead>
<tr>
<th>Images</th>
<th>APPM MSE</th>
<th>Secured APPM MSE</th>
<th>MSE Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lenna</td>
<td>2.604</td>
<td>2.466</td>
<td>0.138</td>
</tr>
<tr>
<td>Jet</td>
<td>2.609</td>
<td>2.466</td>
<td>0.143</td>
</tr>
<tr>
<td>Boat</td>
<td>2.598</td>
<td>2.59</td>
<td>0.008</td>
</tr>
<tr>
<td>House</td>
<td>2.6</td>
<td>2.53</td>
<td>0.07</td>
</tr>
<tr>
<td>Elaine</td>
<td>2.582</td>
<td>2.49</td>
<td>0.092</td>
</tr>
<tr>
<td>Average MSE</td>
<td>2.5986</td>
<td>2.5084</td>
<td>0.0902</td>
</tr>
</tbody>
</table>

The Table 2 shows the performance improvement of Secured APPM technique over the APPM technique. This table shows the performance improvement of MSE and with payload of 3.815 bpp, 2.480 bpp and 1.526 bpp.
7 PERFORMANCE AND SECURITY ANALYSIS

In this section, we analyze the security of Secured APPM under statistical steganalysis schemes, including the HVDH scheme. The HVDH [15] scheme is used to detect the presence of hiding message according to the distance between vertical and horizontal histograms. [15] The proposed a detection method based on the statistical analysis of histogram differences. Zhao et al. [15] observed that for many pair wise embedding methods, the difference between the horizontal difference histograms and vertical difference histograms are significantly altered. Zhao et al. [15] use the distance between $H_h$ and $H_v$ as a statistical detector to detect the abnormality of histogram. [15] The distance is defined as

$$D = \left( \sum_{t=-T}^{T} \left( \hat{H}_h(t) - \hat{H}_v(i) \right)^2 \right)^{\frac{1}{2}}$$

$T$ is a predefined threshold. A larger $D$ indicates that $H_h$ and $H_v$ have larger differences and thus, the image is likely to have messages embedded. [2] The fig.8 shows the security analysis and comparison of histogram of stego and cover images. From these figures we can say that the histogram of cover and stego images are equal. To detect the presence of secret message we employ the security analysis and steganalysis attack on these images but the results produced from them shows that the Secured APPM technique is secure under the detection of some well-known steganalysis techniques.

Fig.8. Security Analysis and Comparison of Cover and Stego Images

8 CONCLUSION AND FUTURE SCOPE

This paper proposed a simple and efficient data embedding method named as Secured APPM based on APPM. In that two pixels are used as an embedding unit and a specially designed compact neighborhood set is used to embed secret message digits in to a smallest possible notational system by allowing users to select digits in any notational system for the data embedding. The proposed method not only resolves the low-payload problem in EMD, but also offers smaller MSE than OPAP, DE and APPM. It also provides a better image quality because Secured APPM does not produce any artifacts in stego images. The steganalysis results of stego images are similar to those of the cover images, which offer a secure communication under adjustable embedding capacity. It also contains additional features such as digital watermark and encryption of secret messages for the provision of more security. The secured APPM technique is also able to hide all different types of data provided to it in languages like English, Marathi, and Hindi etc. As well as this technique is secure under the detection of some well-known steganalysis techniques. All these various features made a Secured APPM technique a straightforward, economical embedding method for the data hiding. In future Secured APPM may have a chance to increase the capacity of data embedding in the cover images of it. Also there may be a chance of little improvement of MSE in it and chance to provide more security.
ACKNOWLEDGMENT

Sincerely thank the all experts who have contributed towards development of this paper.

REFERENCE


AUTHOR

Mr. Swapnil S. Thakare received the B.E. degree in Computer Engineering from University of Pune in 2011. Now he is currently pursuing M.E. (PG) degree in Computer Engineering from University of Pune.

Prof. Niranjan L. Bhale received the B.E. degree in Computer Engineering from Amravati University in 1991 and M. Tech. degree in Computer Engineering from DBATU University in 2006. Currently he is working as Associate professor and Head of Department, Information Technology in MCOERC, Nashik.