CHAPTER 5
MULTILAYER SHELTER APPROACH OF ADAPTIVE K-BIT EMBEDDING FOR BIOMETRIC TEMPLATE PROTECTION

The driving force in the evolution of the digitized world has been in large part due to the development of computer technology and the Internet. This change has given rise to large amounts of data have being created, managed and stored in various digital file formats as well as transmitted through either public or private digital channels (Thomas 2003).

Images can be more than what we see with our Human Visual System (HVS), hence, they can convey more than merely 1000 words. For decades people strove to develop innovative methods for secret communication (Simmons 1984). Multimedia which needs to be secured may conceivably be encoded using cryptography or data hiding techniques including steganography and digital watermarking. Cryptography encodes the confidential data into another form, either meaningful or not (Kahn 1996). A warden observing the communication channel is able to identify if a suspicious file is being transmitted. Steganography and digital watermarking used as means of data hiding techniques are popularly utilized for secure communication as mentioned in Amitava et al (2012). Types of cryptography techniques are categorized by the use of keys as well as pieces of information for extracting the protected file. Digital watermarking protects the multimedia by hiding authentication data either perceptually or inconspicuously while
steganography embeds the secret into another selection of multimedia avoiding visual attacks Bender et al (2000). All three methods are used for privacy and copyright protection, such as authentication of identifying data and intellectual property protection (Hosmer 2006). Steganography also used to transmit electronic patient records (EPR) across distances to hospitals and countries through the Internet. However, since EPR is a highly personal medical documentation, transmission of secure EPR is required to reduce the risk of security breach on the network and prevent accessing of data by unauthorized end-users as in Shaou-Gang Miaou et al (2000), Nirinjan & Anand (1998) and Li et al (2007). The proposed technique also suitable for guaranteed transparency of EPR data.

5.1 INTRODUCTION

Three techniques are interlinked, steganography, watermarking and cryptography (Petitcolas 2000). The first two are quite difficult to tease apart especially for those coming from different disciplines. Figure 5.1 and Table 5.1 may eradicate such confusion. The work presented here revolves around steganography in digital images and does not discuss other types of steganography (such as linguistic or audio).

![Figure 5.1 The different embodiment disciplines of information hiding](image-url)
<table>
<thead>
<tr>
<th>Criterion/Method</th>
<th>Steganography</th>
<th>Watermarking</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Carrier</strong></td>
<td>Any digital media</td>
<td>Mostly image/audio files</td>
<td>Usually text based with some extensions to image files</td>
</tr>
<tr>
<td><strong>Secret data</strong></td>
<td>Payload</td>
<td>Watermark</td>
<td>Plaintext</td>
</tr>
<tr>
<td><strong>Key</strong></td>
<td>Optional</td>
<td></td>
<td>Necessary</td>
</tr>
<tr>
<td><strong>Input files</strong></td>
<td>At least two unless in self-embedding</td>
<td></td>
<td>One</td>
</tr>
<tr>
<td><strong>Detection</strong></td>
<td>Blind</td>
<td>Usually informative (i.e., original cover or watermark are needed for recovery)</td>
<td>Blind</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Full retrieval of data</td>
<td>Usually achieved by cross correlation</td>
<td>Full retrieval of data</td>
</tr>
<tr>
<td><strong>Objective</strong></td>
<td>Secret communication</td>
<td>Copyright preserving</td>
<td>Data protection</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Stego file</td>
<td>Watermarked file</td>
<td>Cipher text</td>
</tr>
<tr>
<td><strong>Concern</strong></td>
<td>Delectability/capacity</td>
<td>Robustness</td>
<td>Robustness</td>
</tr>
<tr>
<td><strong>Types of attacks</strong></td>
<td>Steganalysis</td>
<td>Image processing</td>
<td>Cryptanalysis</td>
</tr>
<tr>
<td><strong>Visibility</strong></td>
<td>Never</td>
<td>Sometimes</td>
<td>Always</td>
</tr>
<tr>
<td><strong>Fails when</strong></td>
<td>It is detected</td>
<td>It is removed/replaced</td>
<td>De- ciphered</td>
</tr>
<tr>
<td><strong>Relation to cover</strong></td>
<td>Not necessarily related to the cover. The message is more important than the cover.</td>
<td>Usually becomes an attribute of the cover image. The cover is more important than the message.</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Flexibility</strong></td>
<td>Free to choose any suitable cover</td>
<td>Cover choice is restricted</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>Very ancient except its digital version</td>
<td>Modern era</td>
<td>Modern era</td>
</tr>
</tbody>
</table>
The basic terminologies used in Steganography are defined as follows.

- **Cover image**: an image in which a message will be hidden within.

- **Stego key**: a parameter used to restrict the parties able to extract the stego message from stego files. Note that the key may be incorporated within the stego file. Certain stego methods require no input key by the user when embedding or extracting the hidden message. This occurs when a stego method embeds the stego message in a sequential manner; otherwise, a form of randomness must be used when embedding the message. A stego method that uses an internal random number generator, the seed used by the generator can be defined as an internal stego key.

- **Stego image/Steganogram**: an image containing a hidden message produced by a steganographic process from stego messages (payload), cover images, and stego keys.

- **Steganalyst**: an analyst that applies steganalysis to a digital file in an attempt to detect and extract the stego data.

### 5.1.1 Steganography Protocols

Practically there are three major categories of steganographic protocols: pure steganography, Secret key steganography and Public key steganography as in Johnson & Jajodia (1998).
Pure-Steganography

The steganography system which does not require prior exchange of a secret key among the communicating parties is called pure steganography. No information is required to start the communication process: the security of the system thus depends entirely on its secrecy. It is the weakest protocol due to the assumption that parties other than the intended ones are not aware of such type of exchange of secret information.

The embedding process can be described as a mapping $E: C \times M \rightarrow C$, where $C$ is the set of possible covers and $M$ the set of possible messages, which is shown in Figure 5.2. The extraction process consists of a mapping $D: C \rightarrow M$, extracting the secret message out of a cover. It is necessary that $|C| \geq |M|$. Both sender and receiver must have access to the embedding and extraction algorithm, but the algorithms should not be public.

![Figure 5.2 Pure Steganography](image)

**Secret-key Steganography**

A secret key steganography system is similar to a symmetric cipher where the sender chooses a cover $c$ and embeds the secret message into $c$ using a secret key $k$, Figure 5.3. If the key used in the embedding process is known to the receiver, he or she can reverse the process and extract the secret message. In general, the secret key is seeded into the Pseudorandom number generator (PRNG) to locate the embedding positions randomly. Anyone who does not know the secret key should not be able to obtain evidence of the
encoded information. Secret key steganography requires the exchange of the key. The advantage lies in the fact that an adversary needs to apply brute force etc. attack to get the secret information out of the cover which require resources such as computational power, time, and determination.

![Diagram of Secret Key Steganography]

**Figure 5.3 Secret Key Steganography**

The secret key steganography can be defined as the quintuple $(C, M, K, DK, EK)$ where:

- **C**: the set of possible covers.
- **M**: the set of secret message.
- **K**: the set of secret keys.
- **EK**: $C \times M \times K \rightarrow C$

With the property that $DK(EK(c, m, k), k) = m$ for all $m \in M$, $c \in C$ and $k \in K$.

**Public-Key Steganography**

As in public key cryptography, public key steganography does not rely on the exchange of a secret key. Public key steganography systems require the use of two keys, one private and one public key. The public key is stored in a public database. The public key is used in the embedding process and
the secret key is used to reconstruct the secret message. Public key steganography utilizes the fact that the decoding function $D$ in a steganography system can be applied to any cover $c$, whether or not it already contains a secret message. Public key Steganography is represented in Figure 5.4.

![Figure 5.4 Public Key Steganography](image)

### 5.1.2 Properties of Steganographic Systems

Steganography, as already mentioned, consists of undetectably altering cover objects to embed a message with the purpose of achieving secret communication (Provos & Honeyman 2003). In contrast, watermarking systems also deal with the embedding of a message in a cover, the watermark, but their ultimate goal is to do so imperceptibly, not to hide the fact that the communication is taking place.

#### a) Embedding Effectiveness

In steganographic systems, most of the constraints are imposed on the extractor, not the embedder. Embedding is not restricted to a particular cover image. Thus, the user or embedder is free to choose the most appropriate cover among all.
b) Fidelity

Because fidelity in watermarking corresponds to the perceptual quality of a watermarked cover, at first it seems irrelevant to steganographic systems. Steganalysis systems operate under the assumption that the attacker does not have access to the original cover image. Therefore, it is impossible for an adversary to determine the existence of a hidden message, if the stego object satisfies undetectability constraints.

c) Embedding Capacity

Embedding capacity in Steganography refers to the amount of information that can be hidden in a cover image, or it is related to the amount of redundant bits present in the medium.

d) Embedding Efficiency

In steganographic systems is often the case that the number of embedding changes applied to a cover object affects the detectability of the hidden message Moulin & Koetter (2005). The smaller the number of changes when embedding, the smaller the chance that a steganalysis method will determine the presence of the message Regarajan et al (2010). That happens because when a cover image exhibits fewer changes; the statistics computed by an adversary are less likely to be disrupted, preventing a successful attack on the system. Hence, if the effect of all embedding modifications is relatively the same, the embedding efficiency is the number of secret message bits embedded per embedding change (Lyu & Farid 2006).
Steganography becomes more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevent the detection of hidden messages. Some of the techniques used in Steganography are domain tools or simple system such as least significant bit (LSB) insertion Khodaei et al (2012), Marghny et al (2011) and Masud et al (2011). The Least Significant Bit (LSB) method directly replaces the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity Chi-Kwong Chan & Cheng (2003). In this work, a Noise based embedding technique by using Salt and Pepper noise is proposed for steganography which is entirely different from the available techniques and the overall architecture is given in Figure 5.5.

5.2 REVIEW OF RELATED RESEARCHES

The approach for Least Significant Bit (LSB) based on image steganography (Medeni et al 2010) enhances the existing LSB substitution techniques to improve the security level of hidden information. It is a new approach to substitute LSB of RGB true colour image. The new security conception hides secret information within the LSB of image where a secret
key encrypts the hidden information to protect it from unauthorized users. In general, in LSB methods, hidden information is stored into a specific position of LSB of image. For this reason, knowing the retrieval methods, anyone can extract the hidden information. The hidden information is stored into different position of LSB of image depending on the secret key. As a result, it is difficult to extract the hidden information knowing the retrieval methods. We have used the Peak Signal-to-Noise Ratio (PSNR) to measure the quality of the stego images. The value of PSNR gives better result because our proposed method changes very small number of bits of the image. The obtained results show that the proposed method results in LSB based image steganography using secret key which provides good security issue and PSNR value than general LSB based image steganography methods.

The modified least significant bit (LSB) substitution method (Masud et al 2011) for data hiding is proposed. Conventional LSB technique uses the least significant bit of consecutive pixels for embedding the message which draws suspicion to transmission of a hidden message. If the suspicion is raised, then the goal of steganography is defeated. Still LSB technique is the most widely used as it is simple. In this implementation pixels to be substituted with information are selected randomly which makes it superior to the conventional approach. The robustness of the algorithm is further increased by using keyless steganography. This paper proposes a novel technique to hide information in a 24 bpp RGB image using modified LSB substitution method. In conventional methods selection of pixels is done in an orderly fashion, usually using a key, whereas in the proposed algorithm selection of pixels to be modified is performed randomly. This makes the algorithm secure than conventional algorithms.

A novel technique for Image steganography based on LSB using X-box mapping (Supriya et al 2012), several Xboxes were used by having
unique data. The embedding part has been done by this Steganography algorithm where the four unique X-boxes used with sixteen different values (represented by 4-bits) and each value is mapped to the four LSBs of the cover image. This mapping provides sufficient security to the payload because without knowing the mapping rules no one can extract the secret data (payload). This approach is better because without stego key, no one can extract the original information from the stego-image, for purposes of secret communication which is more important.

The implementation of two image steganographic techniques shall be implemented in MATLAB (Rengarajan et al 2011). The first is a filter method to embed text information into image and new methods have been demonstrated to increase the information embedding capacity in the same domain. The second method is the wavelet transform method which proves to be more secured than any other method of image steganography. The filter method shows that the embedding capacity can be increased and the wavelet method shows that the security of data is high lightened.

A Novel approach to RGB channel based steganography technique is proposed in Nag et al (2012). The RSA algorithm is used for encryption and decryption. In a RGB image, each pixel (24 bits) is having R-channel 8 bits, G-channel 8 bits and B-channel 8 bits. The image is divided into 8 blocks and the cipher text is divided into 8 blocks. One cipher block is allocated to be embedded in any one image block by a user defined sub key. Out of three channels in each pixel of the image one is used as a indicator channel. The indicator channel for the each block is not same. The other two channels (called data channels) are used for hiding cipher text bits in 4 Least significant bit (LSB) location. In a data channel 4 bits of cipher text can be embedded, if after embedding the change in pixel value is less than or equal to 7. The two LSB of indicator will tell whether the cipher text is embedded in
only one data channel or in both channels, so the retrieving can be done accordingly at the receiver. The technique is implemented and results are analyzed.

Reference table (RT) based embedding method embeds secret digits into pixel pairs under the guidance of a reference table. Most of the existing RT-based methods either require elaborate conversions among different bases, or have limited embedding capacity. Patched reference table (PRT) used as a guide and propose a PRT method to provide a better image quality and extendable embedding capacity. We also exploit the concept of pixel value differencing (PVD) and propose another method PRT–PVD. In the traditional PVD-based methods, the shape of the difference histograms of the stego images is significantly altered and, thus, vulnerable to some steganalysis Wien et al (2012). PRT–PVD adopts the PRT method and uses a specially designed embedding sequence to preserve the difference histogram shape. Experimental results reveal that the proposed PRT and PRT–PVD methods not only have better embedding efficiency over the existing methods, but also are robust to detection by modern steganalysis tools. PRT–PVD considers HVS and exploits the pixel differences to embed different number of bits. The proposed PRT–PVD method is robust to the detection of SPAM, RS scheme, and the histogram analysis. Experimental results show that the proposed PRT and PRT–PVD methods outperform prior RT-based and PVD-based methods in terms of image quality and security.

A new adaptive data-hiding method based on least-significant-bit (LSB) substitution and pixel value differencing (PVD) for grey-scale images. The proposed method partition the cover image into some non-overlapping blocks having three consecutive pixels and select the second pixel of each block as the central pixel (called base-pixel). Then, k-bits of secret data are embedded in the base pixel by using LSB substitution and optimal pixel
adjustment process (OPAP). The difference between the base-pixel value and other pixel values in the block are utilised to determine how many secret bits can be embedded in the two pixels Joan Condell et al (2010). Also, the method divides all possible differences into lower level and higher level with a number of ranges. Then, it obtains the number of the secret bits that will be embedded into each block depending on the range which the difference values belong to. The experimental results show that the proposed method can embed a large amount of secret data while maintaining a high visual quality of the stego-images. The peak signal-to-noise ratio (PSNR) values and the embedding capacity of our method are higher than those of three other data-hiding methods.

The algorithm developed in random image steganography are so well customized, that inclusion of a randomization hints none about the confidentiality, hence giving steganography an upper hand over many other methods of image data hiding. Amirtharajan & Adharsh (2010) proposed a novel steganography technique for digital colour image which achieves the purported targets. The professed methodology employs a complete random scheme for pixel selection and embedding of data. Of the three colour channels (Red, Green, Blue) in a given colour image, the least two significant bits of any one of the channels of the color image is used to channelize the embedding capacity of the remaining two channels. It has been devised into three approaches to achieve various levels of our desired targets. In the first approach, Red is the default guide but it results in localization of MSE in the remaining two channels, which makes it slightly vulnerable. In the second approach, user gets the liberty to select the guiding channel (Red, Green or Blue) to guide the remaining two channels. It will increase the robustness and imperceptibility of the embedded image however the MSE factor will still remain as a drawback. The third approach improves the performance factor as a cyclic methodology is employed and the guiding channel is selected in a
cyclic fashion. This ensures the uniform distribution of MSE, which gives better robustness and imperceptibility along with enhanced embedding capacity. The imperceptibility has been enhanced by suitably adapting optimal pixel adjustment process (OPAP) on the stego covers.

An Adaptive Random (AR) k-bit embedding approach has been attempted to enhance the quality of stego-images. The embedding algorithm principally depends on the nature of the cover image pixels and the data present remains occult. The number of embedded bits is dependent on the differences among the three pixels. Moreover, the MSB of data channel of the RGB planes makes the algorithm obscure by intensifying the randomness to a different scale. The original cover is divided into non-overlapping blocks of equal size. The encrypted confidential data are embedded in each block through four different random walks. The best random walk, which provides the minimum degradation for a particular block, is identified, and is fixed for that block. The decision on the fixed random walk for each block is recorded and kept as the secret key.

The adaptive stego process encrypts confidential data using Data Encryption Standard and randomizes the block selection, employing an intelligent chaotic walk for embedding the encrypted confidential data. The ARIP approach significantly considers the nature of the text while embedding the data, emphasizing the quality enhancement.

### 5.3 PROPOSED APPROACH

In the Recent days, lots of steganography methods have been suggested. They are separated into two classification accomplished on their binding image domains: videolicet, spatial and frequency. In Rengarajan et al (2012), Supriya et al (2012) and Wien et al (2012), the secret entropy are concealed in the pixels of the binding image by applying Least Significant Bit
(LSB), Pixel Value Differencing (PVD), mod, run-length reversible and lossless information concealing based strategies. These strategies have been employed by Gandharba Swain & Saroj Kumar Lenka (2011) to achieve beneficial imperceptibility with a more eminent consignment.

In the frequency domain methods Joan Condell et al (2010), the clandestine information’s are concealed in the transformed coefficients of the binding image, where Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) play the domain converters. Nag et al (2012) suggested fot the spatial domain stego methods, the LSB engraving strategy has been broadly used to conceal clandestine information because of its simplicity and hasten of effectuation, which extends a more eminent concealment capability.

To improve the concealing capacity, more number of clandestine data should be engrafted into all binding image pixels Anita Christaline & Vaishali (2011). Regrettably this scheme abbreviates the lineament of the consequent stego image. Besides the lineament, quantity of information that can be engrafted into an individual binding medium is also very significant.

In our proposed scheme, an adaptive k-bit engraving technique is employed. It meliorates the concealing capacity without conciliatory the quality of the consequence image. In Amirharajan & Adharash (2010), the cyberpunks hacked the stego medium then the chance of capturing the secret information is eminent. But in this proposed scheme it is insufferable; because each pixel in binding image is engrafted with dissimilar number of pixels.

In an existing LSB substitution techniques preprocessing are done by dividing the binding image into blocks, dividing the binding image into
color planes (Medeni 2011), adopting pixel indicator based substitution, Z-scanning, random walk methodology etc, Chan et al (2003) and El-Sayedet al (2012). In our paper, binding image of proposed system is preprocessed by the addition of Salt and Pepper Noise. Noise with defined density is added with the copy of binding image.

This added noise alters the binding image pixel values to either zero if it is added with Salt or Maximum Intensity if it is added with pepper. Finally this noisy image is represented as guiding image.

5.3.1 Enhancement of Proposed System

In this part of research work, the Spatial domain steganography is adopted by employing a Noise guided random stegging with adaptive K- bit embedding for accomplishing eminent concealing capacity without conciliatory the caliber of stego image.

5.3.2 Noise Guided Steging

Salt and Pepper noise is a random noise with ON and OFF Pixels. It modifies the pixel values into either Zero or Maximum intensity of the image. In this proposed scheme Salt and pepper noise is employed for the preprocessing of input binding image. Mostly preprocessing is done for picking out the pixel emplacements of binding image to engraft the clandestine data. If it accompanies any order then the possibility of hacking the secret data is eminent. By the Noise Guided Stegging technique Salt and pepper Noise with determined density is contributed with the input binding image.

Consider a 256*256 size face image of a user is taken as a cover image. One copy of cover image is taken for splitting and then Salt and
Pepper noise is added into this image. After the addition of noise, the image is referred as ‘noisy image’. Now the pixel value in the cover image and the noisy image are differed based on the added noise. The amount of variation in the pixel value of the noisy image can be changed by varying the density of the Salt and Pepper noise. System architecture is shown in Figure 5.6.

![Figure 5.6 System architecture of proposed stegging approach](image)

For example consider the following 4*4 block cover image

<table>
<thead>
<tr>
<th>Cover image (A)</th>
<th>Reference image (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>192 128 136 144</td>
<td>192 0 136 255</td>
</tr>
<tr>
<td>220 123 182 214</td>
<td>255 123 0 255</td>
</tr>
<tr>
<td>180 140 136 194</td>
<td>180 0 255 194</td>
</tr>
<tr>
<td>198 240 220 160</td>
<td>255 240 0 160</td>
</tr>
</tbody>
</table>

In the above example, Salt noise is added with the pixels 2, 7, 10, 15. Similarly Pepper noise is added with pixels 4, 5, 8, 11, 13. The remaining pixels are no noise pixels. The occupation of Salt and Pepper to the particular pixel is varied at every time, because added noise is a random noise.
This noise added binding image is represented as *guiding image* or *reference image* with three dissimilar set of pixels they are Salty pixels, peppery pixels and pure pixels. Corresponding pixels assesses are Zero, Maximum (255 for 256 * 256 images) and similar as like binding image respectively. Instead of fixed decision making for the number of pixels to be engrafted into a binding image, our proposed scheme avails the user defined decision making potentiality. A sender or engrafting authority can decide the pixels should be utilized for engrafting. Sender has the following choices for concealing the clandestine data: select salty pixels of binding image, peppery pixels of binding image, pure pixels of binding image, both salt and pepper, both salt and pure pixels, Pepper and Pure pixels. So the pixels with engrafted clandestine data are extremely insufferable to accumulate because of the randomization of proposed methodology. Eventually this noise guided random stegging system meliorates the quality of the resultant stego image with high imperceptibility factor.

### 5.3.3 Adaptive K-bit Embedding

As mentioned before the quantity of clandestine data that can be engrafted into a single binding image without flexible the lineament of stego image is very significant. To attain this, adaptive K-bit engrafting technique is proposed. Here K alters with the help of random number generator in the range 1 to 4.

It can be easily understand that the pixel value is changed in the noisy image based on the added Salt and Pepper noise. Now the secret data is embed into the cover image based on this changes. That is secret data is embed into the cover image by the varied pixel positions in the reference image. In this proposed method, three different bits of secret data is embedding as per the values in the noisy image.
If the pixel value of noisy image and cover image are same then two bits of data is embed into the cover image. If a pixel is added with salt then that value becomes zero and 1 bit of data is embed. Three bits of data is embedding into the cover image for the pepper added pixel values.

For our convenient a cover image of size 256*256 is taken, therefore the pixel value of salt added portion is 0 and the pixel value of Pepper added portion is 255.

5.4 ALGORITHM FOR PROPOSED METHOD

5.4.1 Algorithm for Embedding Process

1. Read the Cover image.

2. Divide the color Cover image into four Sub images of size.

3. After the cover image is divided into four parts it is further dividing into three planes (Red, Blue and Green Planes).

4. Take a copy of cover image and add Salt and Pepper Noise with Defined density, Mention this as Noisy Image.

5. Compare the pixel values of cover image and Noisy image

6. Add the secret image bits to the cover image based on pixel difference

7. Repeat the process until the entire secret data is embedded into the cover image pixels

8. If the total capacity of cover image pixels is not enough to embed the entire secret data then choose another Cover image.
5.5 SYSTEM DESIGN

![Diagram showing system design process]

Figure 5.7 Proposed system for embedding and retrieving process

System design comprises two contributions such as embedding and retrieving as shown in Figure 5.7. In an embedding part, fused finger print (secret data) and face (cover image) are afforded to the stego system encoder as inputs. Stego system encoder adopts our proposed system for the process of embedding the secret data into the cover image with the support of noisy image. In a retrieving part the reverse process of above is done for acquiring the transmitted clandestine data.

5.5.1 Functional Modules for Engrafting

Algorithm:

Step 1: Get the input from sensor for cover and secret image.

Step 2: Find the binary bit stream of secret image.
Step 3: Interpret the cover image (A) for concealment and subdivide it into 4 images.

Step 4: Add the Salt & Pepper noise with defined Density (Ex: 0.04, 0.06 etc) to the copy of binding image. Name this as noisy image (B)

Step 5: Acquire the noisy image and determine the pixel sets,

If $B = 0$ then Salt pixels ($B_s$),

Else, if $B = 255$, then Pepper pixels ($B_p$)

Else, if $B = A$ then Pure pixels ($B_u$)

Figure 5.8 Information hiding architecture
Step 6:  Done the engrafting through the decision making as follows

If the key for $B_k \neq B_u \neq B_p \neq 0$, then choose the entire binding image and separate them into three sets based on the pixel values.

Else, if the key for $B_k \neq B_u \neq 0 \& B_p = 0$, then choose and separate the pixels of Salt & pure and leave the Pepper pixels in binding image. Else, if the key for $B_k \neq B_p \neq 0 \& B_u = 0$, then choose and separate the pixels of Salty & Peppery and leave the Pure pixels in binding image.

Else, if the key for $B_p \neq B_u \neq 0 \& B_p = 0$, then choose and separate the pixels of peppery & pure and leave the Salty pixels in binding image.

Step 7:  Let us assume all the three pixel sets are chosen for Adaptive K-bit engrafting.

Step 8:  Choose another binding image if the size is not enough to engraft the entire clandestine data bit streams.

Step 9:  Engraft the MSBs of clandestine data bit streams into the LSBs of binding image as mentioned in steps 6&7.

Step 10:  Represent the resultant data engrafted image as Stego image.

Step 11:  Store the resultant image in database.

Procedure done in stego system encoder has explicated in this division. As cited in Figure 5.8, stego system encoder utilizes the proposed schemes, such as split binding, noise guided stegging and adaptive K-bit engrafting. In a preprocessing step Salt and Pepper Noise is added with the binding image. Then the three sets of pixels in the noisy image are used to
lead the adaptive engrafting scheme for concealing the clandestine data into
the binding image as shown in Figure 5.8.

5.5.2 Functional Modules for Retrieving

To retrieve the engrafted clandestine data, Obtained Stego and
Binding images are given as an input to the stego system decoder. Stego
image is divided into three sets as done in stego system encoder. Now, the
exact adaptive key engrafted in stego system encoder must to be given to
retrieve the exact clandestine data as mentioned in Figure 5.9.

![Figure 5.9 Information retrieving architecture](image)
Algorithm:

Step 1: Get the input of face image from user in verification process.

Step 2: Interpret the stego image from Database.

Step 3: Find and separate the emplacement of pixel sets such as Salt, Pepper and pure.

Step 4: Enter the same keys for k1, k2, k3 as entered in the engrafting step.

Step 5: Clandestine data retrieving.

Step 6: Repeat the step-5 for k2 & k3.

Step 7: Combine the data bits retrieved from k1, k2 and k3.

Step 8: Convert the retrieved bits into characters.

Step 9: Give the secret image to ECC point’s generation process.

5.6 TESTING MEASURES

5.6.1 Bits Per Pixels (BPP)

The principal target of this work is to attain eminent concealing capacity over the single binding image. This engrafting capacity is amended by number of bits engrafted into single pixel. This is assessed as follows.

\[
BPP = \left(\frac{C}{P}\right) \quad (5.1)
\]

where,

\(C = \) total number of bits engrafted

\(P = M \times N\)
M = Number of pixels in row of 2D image

N = Number of pixels in column of 2D image

5.6.2 Mean Square Error (MSE)

It is the measure of divergence between the input binding image pixels (A) and consequent stego image pixels (O). A amend system must have lowest MSE.

\[
\text{MSE} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (O_{i,j} - A_{i,j})^2
\]  

(5.2)

where,

M = Number of pixels in row of 2D image

N = Number of pixels in column of 2D image

5.6.3 Peak Signal to Noise Ratio (PSNR)

It is the measure of examining the lineament of the stego image. A amend system must have more eminent PSNR. The system with PSNR around 45-50dB is believed as good system. A system with PSNR above 50dB is conceived as much quality system for a steganography technique.

\[
\text{PSNR} = 10 \log_{10} \left( \frac{I_{\text{max}}}{\text{MSE}} \right) \text{dB}
\]  

(5.3)

\(I_{\text{max}}\) = Maximum intensity of 2D image.

5.7 RESULTS AND DISCUSSION

The experiments were simulated by using CASIA database for fingerprint image and DRIVE dataset for retinal image. The cover image
taken here is retinal and secret image is fingerprint. The obtained results are discussed below.

Figure 5.10 (a) Cover image (b) Stego image

Figure 5.11 Split images
Figure 5.12 Noise binded image

Figure 5.13 Stego image

Figure 5.14 Histogram before hiding for R, G and B plane
Figure 5.15 Histogram after hiding for R, G and B plane

From Figure 5.14 and 5.15, it can be recognized that there is no visual difference between the resultant image and the binding image. The proposed Noise Guided Random Steging with adaptive K-bit engrafting Stego system has been enforced in four sub images. The Capacity of the stego images has been assessed and the consequences are evidenced in Tables 5.2-5.4. Initially, the stego image capacity was gauged by the simple LSB substitution with standardized key engrafting in all the pixels and the consequences are exhibited in Table 5.2. To establish the enhanced concealing capacity and quality of stego image developed by the proposed approach, the estimated BPP, Total engrafting capacity, MSE and PSNR of the stego image are compared with the results presented in Table 5.2.

In Table 5.2 it can be noticed that the concealing capacity and BPP are raised from k=1 to k=4, but values of MSE and PSNR diminished respectively. This fluctuation should not be the case for a amend stego system. A good system must have high concealing capacity as well as superiority stego image. This retreat in the existing simple LSB substitution with standardized key engrafting can be defeat by employing the proposed Adaptive K-bit Engrafting technique.
Tables 5.3-5.4, demonstrates that the proposed scheme has the extremely high data concealing capacity. Adaptive algorithm assures that the quality of the resultant stego image is not compensated.

Table 5.2 BPP, MSE, PSNR, Concealing Capacity of Existing

<table>
<thead>
<tr>
<th>Binding image</th>
<th>Measure</th>
<th>Number of Clandestine Data bits embedded</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>K=1</td>
</tr>
<tr>
<td><strong>User 1</strong></td>
<td>Total No. of Bits embedded</td>
<td>42821</td>
</tr>
<tr>
<td></td>
<td>BPP</td>
<td>0.2178</td>
</tr>
<tr>
<td></td>
<td>MSE</td>
<td>0.3657</td>
</tr>
<tr>
<td></td>
<td>PSNR</td>
<td>62.5657</td>
</tr>
<tr>
<td><strong>User 2</strong></td>
<td>Total No. of Bits embedded</td>
<td>42882</td>
</tr>
<tr>
<td></td>
<td>BPP</td>
<td>0.2181</td>
</tr>
<tr>
<td></td>
<td>MSE</td>
<td>0.0363</td>
</tr>
<tr>
<td></td>
<td>PSNR</td>
<td>62.5741</td>
</tr>
</tbody>
</table>

Table 5.3 Performance measures for User 1

<table>
<thead>
<tr>
<th>Adaptive K-bit K= k1-k2-k3</th>
<th>Total No. of bits Engrafted</th>
<th>BPP</th>
<th>MSE</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-2-3</td>
<td>401230</td>
<td>2.0408</td>
<td>0.2736</td>
<td>52.7179</td>
</tr>
<tr>
<td>3-2-1</td>
<td>400793</td>
<td>2.0385</td>
<td>0.2632</td>
<td>53.7697</td>
</tr>
<tr>
<td>2-1-3</td>
<td>212480</td>
<td>1.0807</td>
<td>0.2470</td>
<td>54.2049</td>
</tr>
<tr>
<td>3-1-2</td>
<td>212319</td>
<td>1.0799</td>
<td>0.2444</td>
<td>54.2495</td>
</tr>
</tbody>
</table>
Table 5.4 Performance measures for User 2

<table>
<thead>
<tr>
<th>Adaptive K-bit K= k1-k2-k3</th>
<th>Total No. of bits embedded</th>
<th>BPP</th>
<th>MSE</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-2-3</td>
<td>402546</td>
<td>2.0475</td>
<td>0.2820</td>
<td>53.6763</td>
</tr>
<tr>
<td>3-2-1</td>
<td>405175</td>
<td>2.0608</td>
<td>0.2017</td>
<td>55.5879</td>
</tr>
<tr>
<td>2-1-3</td>
<td>215248</td>
<td>1.0948</td>
<td>0.2540</td>
<td>54.0854</td>
</tr>
<tr>
<td>3-1-2</td>
<td>216278</td>
<td>1.1000</td>
<td>0.2905</td>
<td>53.5943</td>
</tr>
</tbody>
</table>

The proposed healthy stego system has multilayer shelter against different attacks. For each module, the proposed technique that leads in the maximum BPP, minimum MSE and good PSNR values is adopted here, there by augmenting the concealing capacity of the stego image. Moreover, splicing the binding image with three dissimilar pixel sets by using noise guided image mitrates the protection of the vital message because only the authorized user has the key to the correct compounding of data set pixel emplacements and binary pattern applied in each combination. Furthermore the noise guided stegging technique extends significantly improved security by providing retiring platform for engrafting the information. In addition, choice of engrafting adaptive key and the pixels sets are allowed for user defined decision making instead of manual and predefined decisions. So the attacker can't able to modify or misuse the biometric database.