International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:4, 2014

Biometric Steganography Using Variable Length Embedding

Souvik Bhattacharyya, Indradip Banerjee, Anumoy Chakraborty, Gautam Sanyal

***Abstract*—**Recent growth in digital multimedia technologies has presented a lot of facilities in information transmission, reproduction and manipulation. Therefore, the concept of information security is one of the superior articles in the present day situation. The biometric information security is one of the information security mechanisms. It has the advantages as well as disadvantages. The biometric system is at risk to a range of attacks. These attacks are anticipated to bypass the security system or to suspend the normal functioning. Various hazards have been discovered while using biometric system. Proper use of steganography greatly reduces the risks in biometric systems from the hackers. Steganography is one of the fashionable information hiding technique. The goal of steganography is to hide information inside a cover medium like text, image, audio, video etc. through which it is not possible to detect the existence of the secret information. Here in this paper a new security concept has been established by making the system more secure with the help of steganography along with biometric security. Here the biometric information has been embedded to a skin tone portion of an image with the help of proposed steganographic technique.

***Keywords*—**Biometrics, Skin tone detection, Series, Polynomial, Cover Image, Stego Image.

I. Introduction

IN this extremely digitalized globe, the Internet provides an important responsibility for data transmission and sharing. So therefore the safety and security of communication system is obligatory. The "Information Hiding" is one of the catching focuses for the safety and security. Subsequently the theory of Cryptography [1] and watermarking [2] has been developed. The word "Security" is a very communicable word from prehistoric age and the meaning has been changed in modern age, because the research in reverse engineering techniques has been increased the processing power which rise the fight between researches in cryptanalysis [3] and watermarking detection [4]. To crack these troubles the conception of Steganography [5] has been formed by the researchers. Steganography is one kind of information hiding appliance that can conceal secret information within a normal carrier media, such as text, image, audio, video, protocol etc. Steganography derived from the Greek words, literally means "covered writing". Steganalysis is a challenge to detect the existence and extract the hidden secret message from stego. If the existence of the hidden message is exposed, the goal of steganography is crushed. Fig. 1 describes the types of steganography. Steganography have various techniques. Text Steganography [6] has the categories like Format-based, random & statistical generation, Linguistic methods and Quantum Approach [7]. In audio Steganography [8], messages are embedded into digitized audio signal which result slight alteration of binary sequence of the corresponding audio file. Several new approaches are studied in video data steganography literature [8]. In image steganographic techniques various ways are used, which are as follows [9]:

- Substitution technique in Spatial Domain: In this case the least significant bits of the cover item are replaced without modifying the complete cover image.
- Transform domain technique: Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) are used to hide information in transform coefficients of the cover images.
- Spread spectrum technique: The message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the information.
- Statistical technique: Here the information is encoded by changing various numerical properties of cover image and the message bits are hidden in the block of cover image.
- Distortion technique: Information is stored by signal distortion.
- Pixel Mapping Method (PMM) [10], [11]: Embedding positions are selected by some function and Data embedding are done by mapping each two or four bits of the secret message in each of the neighbor pixel based on some features of that pixel.
- Pixel Factor Mapping (PFM) [12], [13]: Embed the four bits of secret message in a single pixel intensity based on the maximum prime factor value of pixel intensity. It works in spatial and frequency domain with high embedding capacity.

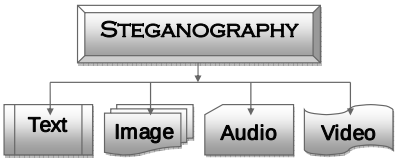


Fig. 1 Types of Steganography

Automatic recognition system of an individual has been derived from the physiological and behavioral [14]–[19] characteristic which describes the Biometric security system. The term "biometrics" is derived from a Greek words bio means "life" and metric means "to measure". Biometric

Souvik Bhattacharyya and Anumoy Chakraborty are with the University Institute of Technology, The University of Burdwan, Burdwan (e-mail: souvik.bha@gmail.com, anu_chak62@yahoo.co.in).

Indradip Banerjee and Gautam Sanyal are with the National Institute of Technology, Durgapur, West Bengal, India. (e-mail: indradip.banerjee@yahoo.com, nitgsanyal@gmail.com)

systems ascertain a person's identity based on pattern analyses carried out on specific human traits [15], [16]. Physiological based biometric systems consist of fingerprints, retina, iris, hand geometry, hand vein, ear shape and facial recognition systems [17]. These features are typically unchangeable exclusive of causing disturbance to human being. On the other hand, behavioural biometric characteristics are later stabilizing over a period of time. Some of the examples of behavioural-based biometric systems are voice recognition, keystroke dynamics, signature verification and gait analysis. In case of a bank card, the biometric data can be used because there are a finite number of substitutes for a person i.e. as a person has only 10 fingers, two eyes, etc. Certifying the privacy and security of biometric data, users will be doubtful to accept the technology if information could hypothetically be tampered with, stolen or misused. [18]. Generations wise biometric techniques have been well-appointed in [19]. Fig. 2 describes the classification of biometric techniques. In existing system there are various methods have been developed by most of the researchers using different biometric features.

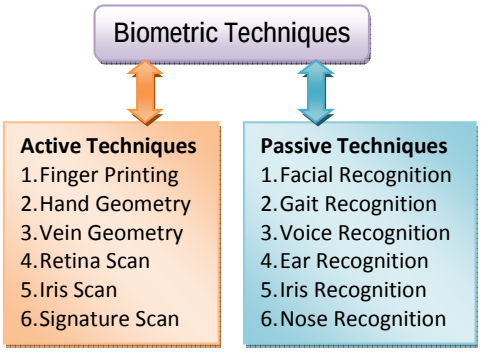


Fig 2 Classification of biometric techniques

This is a new steganography technique apart from the other steganographic techniques. In this work the biometric thumb image is embedded to a skin tone portion of an image as bit stream of two to four bits combinations. The pixel selection technique is to find out the skin tone portion from the cover image. This method can also extract biometric information even after noise addition in stego image. The developed contribution is a novel biometric steganography technique. Rest of the paper has been organized as following sections: Section II describes some related works on image steganography. Section III deals with proposed method and Section IV are for algorithms. In Section V experimental results are discussed and analyzed mathematically. Section VI makes a comparison and Section VII draws the conclusion.

II. Associated Work

A. Image Steganography Techniques

The image steganography can be possible in two domains, one is Spatial and another is frequency domain. There are various techniques and modules developed by different researchers. Some of them are discussed below:

1) Spatial Domain Technique

The common techniques in this domain is least-significant-bit (LSB) [20] where directly replace the LSBs of the cover-image with message bits. The pixel-value differencing (PVD) method proposed by Wu and Tsai [21] can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image. Among them Chang et al. [22] proposes a new method using tri-way pixel-value differencing which is better than original PVD method with respect to the embedding capacity and PSNR. In 2004, Potdar et al. [23] proposes GLM (Gray level modification) technique which is used to map data by modifying the gray level of the image pixels. Hong and Chen [24] introduced a new method based on pixel pair matching (PPM).

2) Frequency Domain Technique

In data hiding based on JPEG [25] method, the cover image is broken down into a set of blocks and performed the discrete cosine transform (DCT) on each block. The transformed coefficients are quantized with the help of default quantization table of JPEG. The secret data is embedded into the quantized coefficients. Kobayashi et al. [26] embed one secret bit into one 8×8 DCT block. Jpeg–Jsteg [27], the secret data is embedded into the LSB of the quantized DCT coefficients whose values are not 0, 1, or −1. Mutto and Kumar proposed a Jpeg-Jsteg algorithm based on T-codes, which are belongs to the families of variable-length codes (VLC) that exhibit extraordinarily strong tendency towards self synchronization. The concepts of simple Tcodes were given by M.R. Titchner [28]. K. B. Raja et al. [29] embedded in the wavelet coefficients of the cover image. Radovan Ridzon et al. [30] presented a technique to hide secret information inside the cover image. Chang et al. [31] embed the secret data into the middle frequency part of the quantized DCT coefficients.

B. Biometric Information Security:

Biometrics system intends to recognize an individual through physiological or behavioral attributes, for instance face, fingerprint, iris, retina and DNA also [32]. In biometric technique there are various ways and all biometric techniques differ according to security level, user acceptance, cost and performance. Some of the techniques are describe below:

1) Fingerprints

Fingerprint [33] is one of the biometric securities, which is based on fingertip pattern recognition. There are three basic patterns of fingerprint ridges: 1) Arch: Ridges enter from one side of the finger, forming in the center and exit the other side of the finger. 2) Loop: Ridges enter from one side of a finger then form a curve and then exit on that same side. 3) Whorl: The ridges form circularly around a central point on the finger. There are several approaches to fingerprint verification. Some of them follow the conventional method of matching finer points; others use straight pattern matching mechanism. Some of fingerprint verification approaches can detect a live finger where as some cannot. Various fingerprint devices are available than any other biometric system. Scientists have found that family members are inherited patterns, so they

often share the same general fingerprint patterns.

2) Retina

Analyzing the complex structure of the capillaries that is the layer of blood vessels at retina which is not entirely genetically determined i.e. back of eye is involved in this procedure. For that reason each person's retina is unique. Find out the unique patterns of the retina using low intensity light source through an optical coupler is the process to identify. The technology can work well but it is not convenient if human uses glasses or having close contact with the reading device [34]. The Advantages in this technique is Low rates of false positives and false negative. This technique is highly reliable because no two people have the same retinal pattern. But the measurement accuracy affected by various eye diseases like cataracts, diabetes and glaucoma or retinal degenerative disorders.

3) Face

Face biometry [35] depending on analyzing facial characteristics. It involves a digital camera to grow a facial image of the user for authentication. In this system it automatically identifying or verifying a person from an image. One of the ways to do this is to compare some selected facial features from the image and a facial database. Among the different biometric techniques, facial recognition may not be the most reliable and efficient.

4) Hand Geometry

In this mechanism the shape of the human hand is computed and analyzes [36]. Hand geometry is based on the palm and fingers structure, width of the fingers in different places, length of the fingers, thickness of the palm area, etc. while these measurements are not very distinctive among people, so hand geometry be capable for identity verification, i.e. personal authentication. This biometric system recommends a good stability of performance characteristics and is reasonably straightforward to apply. This is suitable where lots of users are there in the system and they access infrequently. In this system the accuracy level is very high and performance is flexible.

5) Nose

The nose biometric technique [37] works through features extracting from a nose and by the help of various classification techniques. Geometric ratios and nose ridge shape both demonstrate the procedures of nose's biometric. The nose's biometric is largely unknown and for that reason it is very flexible in performance but the recognition procedure is currently far lower than other biometrics.

6) Ear

One of interesting authentication technique is ear biometric security. Analyzing ear shape and area measurement of a human can identify people [38]. Ear biometrics appears as a well-organized biometric method for human identification and could be used like other biometrics because the human ear goes through little changes as course of age. Now a day the 2D and 3D domain are presented in this biometric feature.

7) Signature

Signature recognition is one of the behavioural biometric systems. Signature signing features like writing speed, velocity and pressure are used for identifications. Signature verification devices are logically accurate in operation and lend themselves to applications where a signature is an accepted identifier [39]. It can be operated in two different ways:

- Static: Users write their signature on paper then digitize through a scanner or camera and the biometric system recognizes the signature analyzing its shape.
- Dynamic: Users write their signature in a digitizing tablet.

8) Iris

In this iris-based biometric [40], the system can analyzing features using mathematical pattern-recognition techniques. It stores the measurement of the colored ring of tissue surrounds the pupil of eye. Iris biometrics uses a fairly conventional camera element and obliges no close contact among the user and reader. In this system, first localize the inner and outer boundaries of the iris (pupil and limbus) from an eye image. Then detect and exclude eyelids, eyelashes and specular reflections that often unused parts of the iris. The set of pixels contain the iris, normalized by a rubber-sheet model to compensate for pupil dilation or constriction, then analyzed to extract bit pattern information which is needed for compare of two iris images. This system work with glasses and few devices can work well in identification mode also.

9) Voice

Voice biometrics [41] has the most probable for enlargement, because it requires no new hardware—most PCs already contain a microphone. Speaker recognition is the identification of the human beings that who is speaking. By the help of characteristics of their voices the verification process occurs. But the noisy voice can affect verification.

10) Vein geometry

In this technique the vein of hand, vein of finger, vein of palm etc are used for authentication purpose. It is not observable under visible light so the security is very high. The infrared sensors used for captured and detect the structure of the vein patterns. There are two kinds of imaging technology have been used to develop this system, which are Far-infrared (FIR) and Near-infrared (NIR). Visibility of the vein structure depends on different issues like age, thickness of the skin, ambient temperature, physical activity, depth of the veins under the skin. Additionally, skin texture for instance moles, warts, scars and hair can also distress the imaging excellence of the veins. L. Wang et al. [42] proposed a verification system of human beings using the thermal-imaged vein pattern in the back of hand. A. Kumar et al. [43] presents a technique which can authenticate a person based on minutiae matching of vein junction points.

III. Proposed Method

In this contribution a spatial domain steganographic technique has been developed for embedding biometric information in bit stream format. This procedure is describing in details with the habit of several fragments.

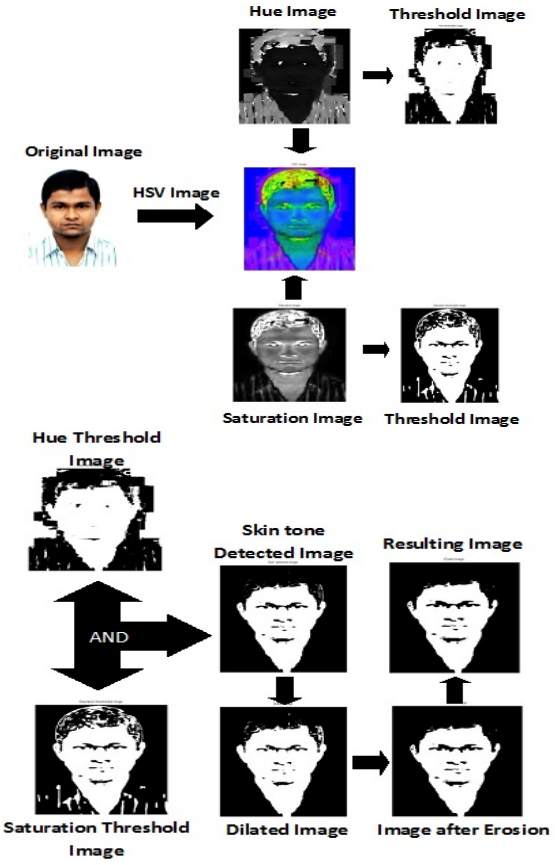


Fig. 3 Technique of Pixel Selection

A. Pixel Selection

To select the embedding pixel of the cover image, the biometric algorithm has been used. Through this steganographic system the PSNR value is comparatively better because some special portion of image is used for embedding instead of embedding data anywhere in the image. In this system the skin region of the image has been used for embedding of secret data. There are mainly two kinds of color spaces are suitable for biometric operations which are HSV (Hue, Saturation and Value) and YCbCr (Yellow, Chromatic Blue, Chromatic Red) spaces. The system detects the skin color with the help of skin detector and skin classifier. Skin detector can convert the RGB color space into appropriate color space HSV, as because it is more related to human colour perception. For skin detection a threshold should be chosen as the purpose of hue_range=[h_1,h_2] and sat_range=[S_1,S_2]. Then skin classifier classifies the pixels in the cover image to skin and non skin pixels by defining a boundary. The skin detection algorithm produces a mask which is simply a black and white pixel with the help of threshold, which has a predefined range associated with the target skin pixel values. Most of the researchers are using the threshold as hue_range=[0,0.11] and sat_range=[0.2,0.7]. Fig. 3 illustrates the pixel selection process. After getting the Hue thresholded image and Saturation thresholded image the system perform simple AND operation to detect the skin tone by white marked pixels other pixels are black as it is seen in the Fig. 3. After getting the skin tone detected image the system can remove noise by a morphological filter performing two operations such as Dilation and Erosion. Dilation means expand the skin regions to detect imperfections. Then erosion operation will remove the imperfection to get a better resulting image. Thus the system results the noise free skin tone detected image and continue its operation for further processing.

B. Embedding Space Selection:

In this performance the system follows embedding space varies from pixel to pixel. To get the embedding space of a pixel of the cover image the system uses a series of integers and thus the system adds the squared value of integers up to the below next value $\boldsymbol{\alpha_{ij}}$ of the pixel $\boldsymbol{Pix_{ij}}$ and also do the same up to the next above value $\boldsymbol{\beta_{ij}}$ of the pixel $\boldsymbol{Pix_{ij}}$. As for example, $Pix_{ij} = 127$

Then, $\alpha_{ij} = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 = 91 \langle 127$ and $\beta_{ij} = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 + 7^2 = 140 \rangle 127$.

Then the system calculate the mid value by

$$\gamma_{ij} = \left(\alpha_{ij} + \beta_{ij}\right) / 2 \tag{1}$$

and if $\boldsymbol{Pix_{ij}}$ is less than or equal to the mid value $\boldsymbol{\gamma_{ij}}$ then it get the subtracted value

$$\delta_{ij} = \left(Pix_{ij} - \alpha_{ij}\right) \tag{2}$$

else

$$\delta_{ij} = \left(\beta_{ij} - Pix_{ij}\right) \tag{3}$$

as embedding space. Thus after getting the embedding space for each pixel $\boldsymbol{Pix_{ij}}$ the system will further approach for embedding. Fig. 4 determines the embedding space.

C. Embedding:

To make the steganalysis difficult, this method does not embed the message bit directly to the image and it is done with the help of polynomial functions. Then the value getting from the polynomial is embedded into those pixels of the cover image according to its availability of embedding space.

For a bit stream Bit_s=1010111 the embedding procedure is shown in Fig. 5.

The embedding polynomial used here is as follows:

$$\sum = x^n\left(k+bit_1\right)+x^{n-1}\left(k+bit_2\right)+x^{n-2}\left(k+bit_3\right)+...+x\left(k+bit_n\right) \tag{4}$$

where, bit_n=n^{th} bit of remainder bit stream. Thus the system embed the bit stream according to every pixels embedding

space δ_{ij} and if there is not enough embedding space δ_{ij} then the system go for next pixel of the plane and if data is fully embedded in that plane then the system perform embedding in next plane.

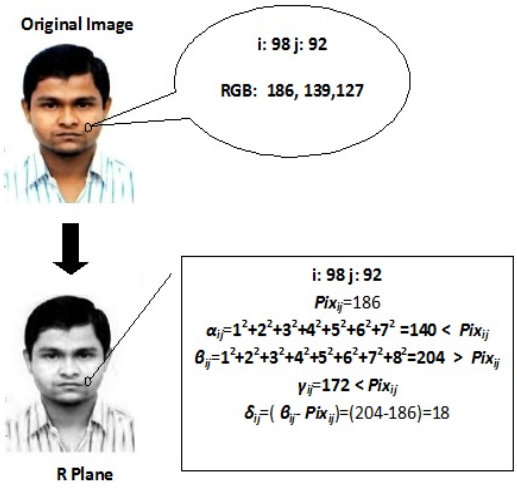


Fig. 4 Determination of embedding space

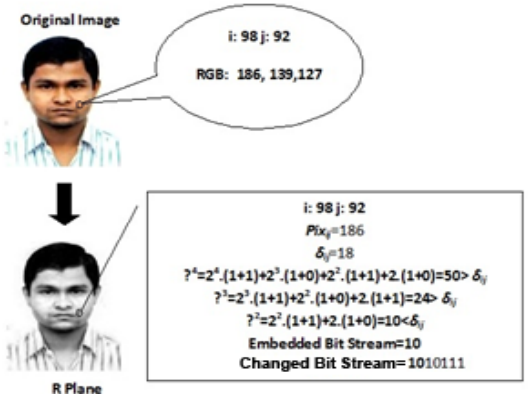


Fig. 5 Embedding procedure

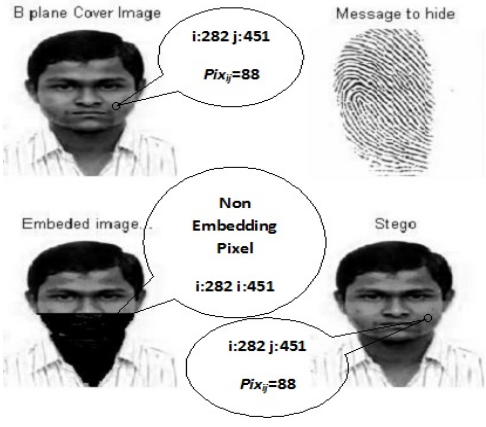


Fig. 6 Non Embedding positions

D.Non Embedding Portion:

The system does not incorporate any stop bit to denote the end of bit stream embedding. One pixel can have a value which falls in much difference from other pixels. But the system sets the value of non embedding pixels in such a manner so that its difference from original cover pixel is one or zero as well as there no data can be extracted at the extraction time. Fig. 6 shows the non embedding positions. Fig. 7 illustrates that how to make the Stego from the cover image and Extract the secret Image.

E. Variable Length Message Embedding:

The system embed a variable length message bits depending upon the availability of embedding space and bit stream also so that those bits of message bit stream is embedded for which $\sum^{n}$ is less than δ_{ij}.

$$\gamma_{ij} = \left(\alpha_{ij} + \beta_{ij}\right)/2 \tag{5}$$

if $Pix_{ij} \le \gamma_{ij}$,where Pix_{ij} is the pixel intensity and δ_{ij} is the embedding space.

$$\delta_{ij} = \left(Pix_{ij} - \alpha_{ij}\right) \tag{6}$$

else

$$\delta_{ij} = \left(\beta_{ij} - Pix_{ij}\right) \tag{7}$$

$$\sum^{n} = x^{n}\left(k+bit_1\right)+x^{n-1}\left(k+bit_2\right)+x^{n-2}\left(k+bit_3\right)+...+x\left(k+bit_n\right) \tag{8}$$

where, bit_n=n^{th} bit of remainder bit stream.

Some of the following cases have been presented below with respect to variable message bit stream 's'-

Case 1:

For a bit stream s=11010110111….

$Pix_{ij} = 173$

Embedding Space $\delta_{ij} = 31$.

$$\sum^{4} = 2^{4}(1+1)+2^{3}(1+1)+2^{2}(1+0)+2\ (1+1) = 56 \rangle \delta_{ij}$$

$$\sum^{3} = 2^{3}(1+1)+2^{2}(1+0)+2\ (1+1) = 24 \langle \delta_{ij}$$

Embedded Bit Stream=110

Changed Bit Stream=1101010111

$Pix_{ij} = 186$

Embedding Space $\delta_{ij} = 18$

$$\sum^{4} = 2^{4}(1+1)+2^{3}(1+0)+2^{2}(1+1)+2\ (1+0) = 50 \rangle \delta_{ij}$$

$$\sum^{3} = 2^{3}(1+1)+2^{2}(1+0)+2\ (1+1) = 24 \rangle \delta_{ij}$$

$$\sum^{2} = 2^{2}(1+1)+2\ (1+0) = 10 \langle \delta_{ij}$$

Embedded Bit Stream=10

Changed Bit Stream=1101010111

$Pix_{ij} = 138$

Embedding Space $\delta_{ij} = 2$

$\sum^4 = 2^4(1+1)+2^3(1+0)+2^2(1+1)+2\ \ (1+1) = 52 \rangle \delta_{ij}$

$\sum^3 = 2^3(1+1)+2^2(1+0)+2\ \ (1+1) = 24 \rangle \delta_{ij}$

$\sum^2 = 2^2(1+1)+2\ \ (1+0) = 10 > \delta_{ij}$

$\sum^1 = 2\ \ (1+1) = 4 \rangle \delta_{ij}$

Embedded Bit Stream=Null
Changed Bit Stream=1101010111

Case 2:

For a bit stream s=1001001101….

$Pix_{ij} = 173$

Embedding Space $\delta_{ij} = 31$

$\sum^4 = 2^4(1+1)+2^3(1+0)+2^2(1+0)+2\ \ (1+1) = 48 \rangle \delta_{ij}$

$\sum^3 = 2^3(1+1)+2^2(1+0)+2\ \ (1+0) = 22 \langle \delta_{ij}$

Embedded Bit Stream=100
Changed Bit Stream=1001011101

$Pix_{ij} = 186$

Embedding Space $\delta_{ij} = 18$

$\sum^4 = 2^4(1+1)+2^3(1+0)+2^2(1+1)+2\ \ (1+1) = 52 \rangle \delta_{ij}$

$\sum^3 = 2^3(1+1)+2^2(1+0)+2\ \ (1+1) = 24 \rangle \delta_{ij}$

$\sum^2 = 2^2(1+1)+2\ \ (1+0) = 10 \langle \delta_{ij}$

Embedded Bit Stream=10
Changed Bit Stream=10010000111

$Pix_{ij} = 138$

Embedding Space $\delta_{ij} = 2$

$\sum^4 = 2^4(1+0)+2^3(1+0)+2^2(1+1)+2\ \ (1+1) = 36 \rangle \delta_{ij}$

$\sum^3 = 2^3(1+0)+2^2(1+0)+2\ \ (1+1) = 16 \rangle \delta_{ij}$

$\sum^2 = 2^2(1+0)+2\ \ (1+0) = 6 \rangle \delta_{ij}$

$\sum^1 = 2\ \ (1+0) = 2 = \delta_{ij}$

Embedded Bit Stream=0
Changed Bit Stream=1001000111

Thus from **Case 1** and **Case 2** it is seen that the system embed a bit stream of length 5 for **Case 1** and of length 6 for **Case 2**. Hence it can conclude that the system embed a variable length message bit stream when bit stream is varied and embedding space $\boldsymbol{\delta_{ij}}$ remains same.

Now the author present variable length message embedding with respect to Embedding Space $\boldsymbol{\delta_{ij}}$.

Case 3:

For a bit stream s=11010110111….

$Pix_{ij} = 173$

Embedding Space $\delta_{ij} = 31$.

$\sum^4 = 2^4(1+1)+2^3(1+1)+2^2(1+0)+2\ \ (1+1) = 56 \rangle \delta_{ij}$

$\sum^3 = 2^3(1+1)+2^2(1+1)+2\ \ (1+0) = 26 \langle \delta_{ij}$

Embedded Bit Stream=110
Changed Bit Stream=1101010111

$Pix_{ij} = 186$

$\delta_{ij} = 18$

$\sum^4 = 2^4(1+1)+2^3(1+0)+2^2(1+1)+2\ \ (1+0) = 50 \rangle \delta_{ij}$

$\sum^3 = 2^3(1+1)+2^2(1+0)+2\ \ (1+1) = 24 \rangle \delta_{ij}$

$\sum^2 = 2^2(1+1)+2\ \ (1+0) = 10 \langle \delta_{ij}$

Embedded Bit Stream=10
Changed Bit Stream=11010110111

$Pix_{ij} = 138$

$\delta_{ij} = 2$

$\sum^4 = 2^4(1+1)+2^3(1+0)+2^2(1+1)+2\ \ (1+1) = 52 \rangle \delta_{ij}$

$\sum^3 = 2^3(1+1)+2^2(1+0)+2\ \ (1+1) = 24 \rangle \delta_{ij}$

$\sum^2 = 2^2(1+1)+2\ \ (1+0) = 10 \rangle \delta_{ij}$

$\sum^1 = 2\ \ (1+1) = 4 \rangle \delta_{ij}$

Embedded Bit Stream=Null
Changed Bit Stream=1101010111

Case 4:

For a bit stream s=1101010010…

$Pix_{ij} = 187$

Embedding Space $\delta_{ij} = 17$

$\sum^4 = 2^4(1+1)+2^3(1+1)+2^2(1+0)+2\ \ (1+1) = 56 \rangle \delta_{ij}$

$\sum^3 = 2^3(1+1)+2^2(1+1)+2\ \ (1+0) = 26 \rangle \delta_{ij}$

$\sum^2 = 2^2(1+1)+2\ \ (1+1) = 12 \langle \delta_{ij}$

Embedded Bit Stream=11
Changed Bit Stream=1101010111

$Pix_{ij} = 185$

$\delta_{ij} = 19$

$\sum^4 = 2^4(1+0)+2^3(1+1)+2^2(1+0)+2\ \ (1+1) = 40 \rangle \delta_{ij}$

$\sum^3 = 2^3(1+0)+2^2(1+1)+2\ \ (1+0) = 18 \langle \delta_{ij}$

Embedded Bit Stream=010
Changed Bit Stream=1101010111

$Pix_{ij} = 160$

$\delta_{ij} = 20$

$\sum^4 = 2^4(1+1)+2^3(1+0)+2^2(1+1)+2\ \ (1+1) = 52 \rangle \delta_{ij}$

$\sum^3 = 2^3(1+1)+2^2(1+0)+2\ \ (1+1) = 24 \rangle \delta_{ij}$

$\sum^2 = 2^2(1+1)+2\ \ (1+0) = 10 \langle \delta_{ij}$

Embedded Bit Stream=10
Changed Bit Stream=1101010111

Thus from **Case 3** and **Case 4** it is seen that the system embed a bit stream of length 5 for **Case 3** and of length 7 for **Case 2**. Hence it can conclude that the system embed a variable length message bit stream when bit stream is fixed and embedding space $\boldsymbol{\delta_{ij}}$ varied.

IV. Algorithms

A. Pixel Selection Algorithm by Skin Tone Detection:

1) Read the cover image
2) Convert the cover image into HSV colour space
3) Get the Hue Image Plane and Saturation Image Plane
4) Threshold the hue image plane and saturation image plane by setting the threshold hue_range = [0,0.11] and sat_range = [0.2,0.7] respectively.
5) Make AND operation between hue thresholded image and saturation thresholded image to get the skin tone detected image.
6) Make Dilation on the resulting image and then Erosion for noise removing.
7) Get the resulting skin tone detected image with white pixel at skin tone detected area otherwise black pixel at non skin tone detected area.

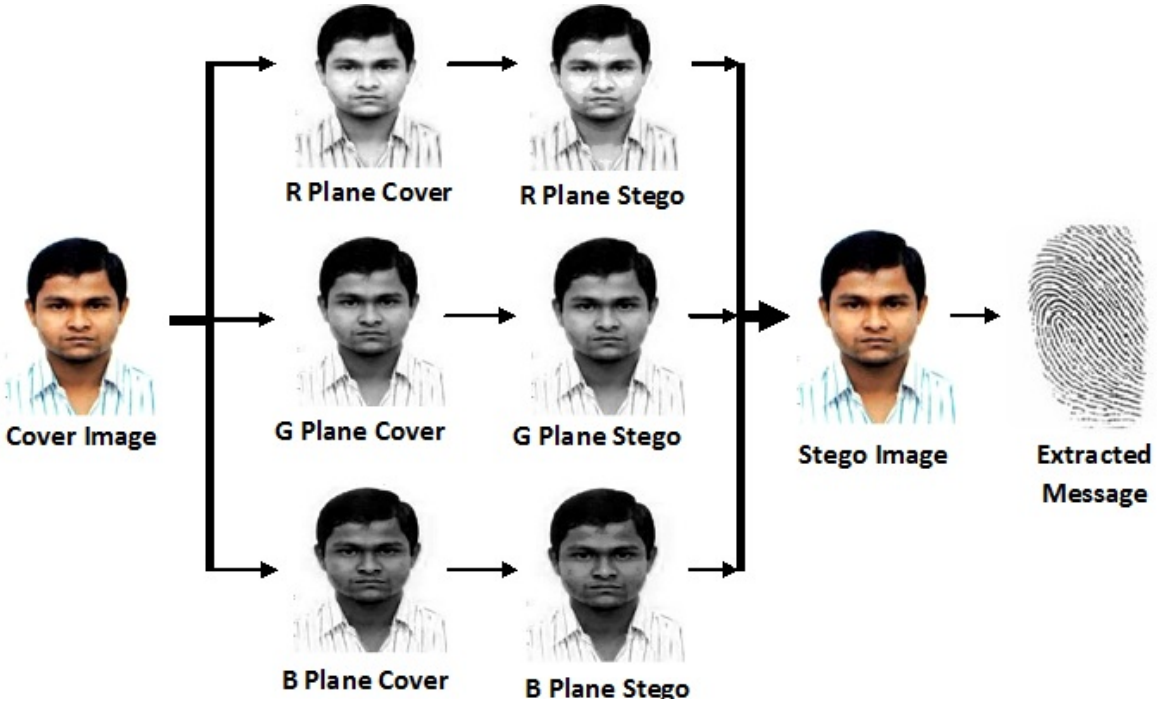


Fig. 7 Resulting Stego and Extracted Image

B. Algorithm for Embedding:

At first convert the message image into a bit stream for embedding.

For an M X N image
for i=1:M
for j=1:N

For each pixel Pix_{ij} in Original image:-

1) α_{ij}:=Add the squared value of integers up to the sum value which is below next of Pix_{ij} value
2) β_{ij}:=Add the squared value of integers up to the sum value which is next above of Pix_{ij} value
3) $\gamma_{ij} = (\alpha_{ij} + \beta_{ij})/2$;
4) if $Pix_{ij} \le \gamma_{ij}$ then $\delta_{ij} := (Pix_{ij} - \alpha_{ij})$ else $\delta_{ij} := (\beta_{ij} - Pix_{ij})$
5) Calculate the value for bit stream of length n= 4,3,2 and 1

$$\sum^{n} = x^{n}(k+bit_1) + x^{n-1}(k+bit_2) + x^{n-2}(k+bit_3) + ... + x(k+bit_n) \quad (9)$$

6) if $\sum^{4} \le \delta_{ij}$ then $\mu_{ij} := \sum^{4}$
elseif $\sum^{3} \le \delta_{ij}$ then $\mu_{ij} := \sum^{3}$
elseif $\sum^{2} \le \delta_{ij}$ then $\mu_{ij} := \sum^{2}$
elseif $\sum^{1} \le \delta_{ij}$ then $\mu_{ij} := \sum^{1}$
7) if $Pix_{ij} \le \gamma_{ij}$ then $S_{ij} := \alpha_{ij} + \mu_{ij}$ else $S_{ij} := \beta_{ij} - \mu_{ij}$;
end j
end i
Stego image S generates.

C. Algorithm for Extraction:

For an M X N Stego Image
for i=1:M
for j=1:N
For each pixel Pix_{ij} in Original image:-

1) α_{ij}:=Add the squared value of integers up to the sum value which is below next of Pix_{ij} value
2) β_{ij}:=Add the squared value of integers up to the sum value which is next above Pix_{ij} value
3) $\gamma_{ij} := (\alpha_{ij} + \beta_{ij})/2$

4) if $S_{ij} \le \gamma_{ij}$ then $\delta_{ij} := (S_{ij} - \alpha_{ij})$ else $\delta_{ij} := (\beta_{ij} - S_{ij})$
5) Get the equivalent bit stream of δ_{ij} and go for next pixel.
6) σ_{ij}=bit stream
Extracted image is σ .

D. Algorithm for Non Embedding Portion:

For an M X N Image
for i=1:M
for j=1:N
1) If the pixel value Pix_{ij} is an odd number
if $Pix_{ij} \le \gamma_{ij}$
if α_{ij}= even
Pix_{ij} unchanged
else if α_{ij}= odd
Pix_{ij} to next even number
elseif $Pix_{ij} > \gamma_{ij}$
if β_{ij} =even
Pix_{ij} unchanged
elseif β_{ij} =odd
Pix_{ij} to below next even number
2) If the pixel value Pix_{ij} is an even number :-
if $Pix_{ij} \le \gamma_{ij}$
if α_{ij}= even
Pix_{ij} to next odd number
else if α_{ij}= odd
Pix_{ij} unchanged
elseif $Pix_{ij} > \gamma_{ij}$
if β_{ij} =even
Pix_{ij} to below next odd number
elseif β_{ij} =odd
Pix_{ij} unchanged

V. Mathematical Analysis

In this segment the experimental results of the method has been described based on some techniques to evaluate the hiding performance. Since the capacity of hiding data depends upon the bit stream want to embed and embedding space depends upon the pixel value so that capacity varies from message to message thus different message image and imperceptibility of the stego image, these two techniques is used here for performance metric. Imperceptibility of the image is called the quality of image. The quality of stego image produced by the proposed method has been tested thoroughly based on various image similarity metrics namely MSE, PSNR, CORELATION, RMSE, SSIM, KL DIVG and ENTROPY. Figs. 10 to 16 show the graphical representation of calculated value of various similarity metrics for images. Various Techniques used to manage the difference between pixels. The techniques are described below:

A. Mean Square Error (MSE):

It is computed by averaging the squared intensity of the cover and stego image pixels. Equation (10) shows the MSE [44].

$$MSE = \frac{1}{NM}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}e(m,n)^2 \quad (10)$$

where NM is the image size (N x M) and e(m,n) is the reconstructed image.

B. Peak Signal-to-Noise Ratio (PSNR):

A mathematical measure of image quality is Signal–to-noise ratio (SNR), which is based on the pixel difference between two images. The SNR measure is an estimate of quality of Stego image compared to cover image. PSNR [44] is shown in (11):

$$PSNR = 10\log_{10}\frac{S^2}{MSE} \quad (11)$$

where, S stands for maximum possible pixel value of the image. If the PSNR is greater than 36 DB then the visibility looks same in between cover and stego image, so HVS not identified the changes.

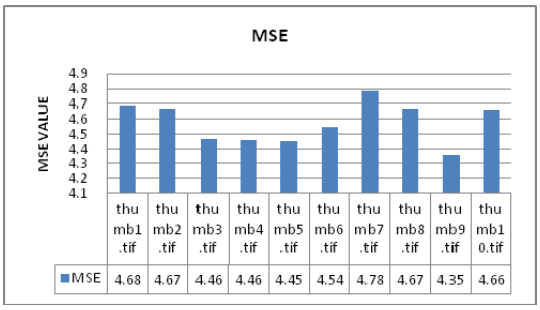


Fig. 8 MSE for various Secret Images

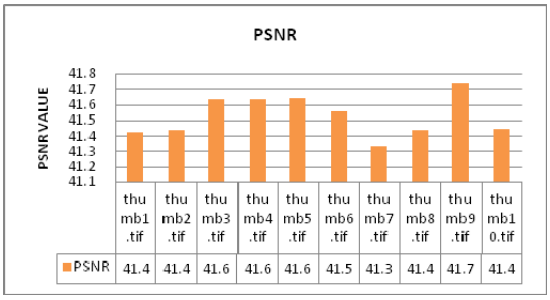


Fig. 9 PSNR for various Secret Images

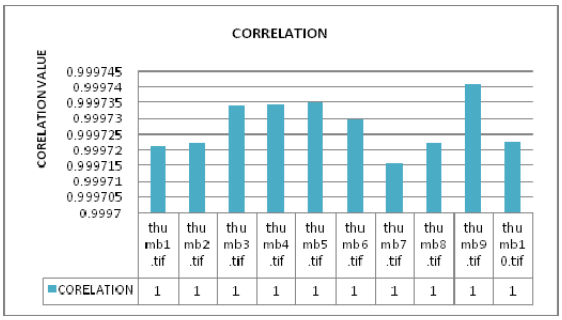


Fig. 10 Correlation for various Secret Images

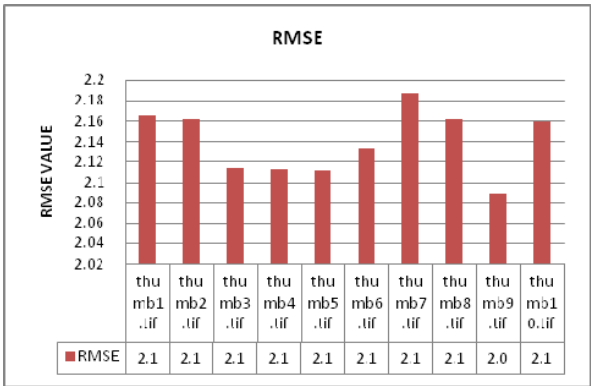


Fig. 11 RMSE for various Secret Images

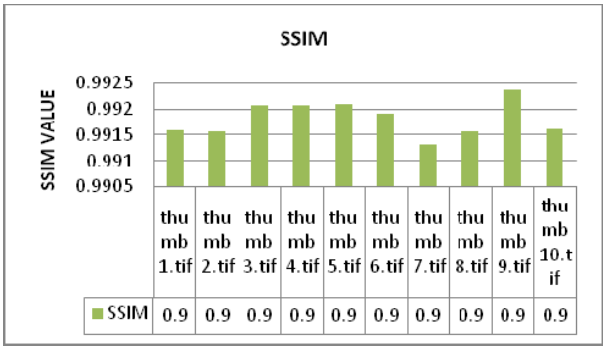


Fig. 12 SSIM for various Secret Images

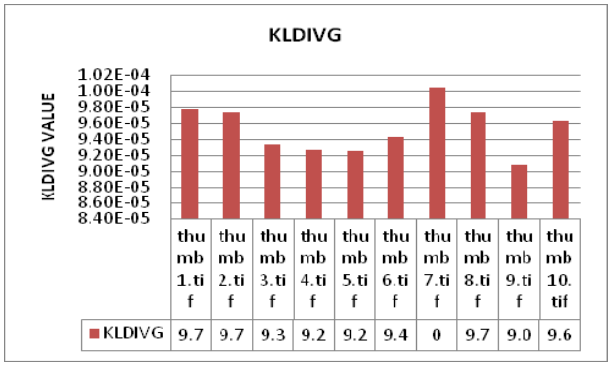


Fig. 13 K L Divergence for various Secret Images

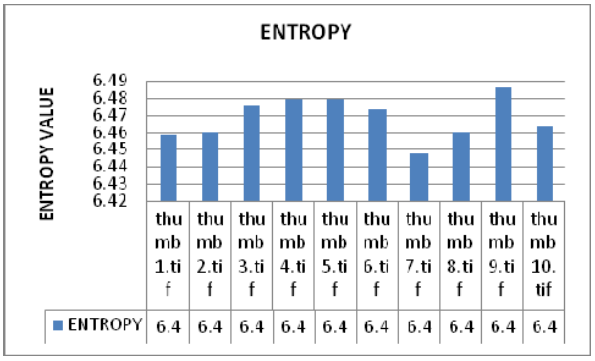


Fig. 14 Entropy for various Secret Images

C. Correlations:

Pearson's correlation coefficient [45] is widely used in statistical analysis as well as image processing. Here apply it in Cover and Stego images to see the difference between these two images. The Correlation shows in (12).

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})\cdot(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \cdot \sum_{i=1}^{n}(y_i - \bar{y})^2}} \quad (12)$$

The Xi and Yi are the cover image and bar of X and Y are stego image positions. The correlation values are tens to 1 that means both the images are likely to same.

D. Root Mean Square Error (RMSE):

RMSE [46] is one kind of measurement of difference between values of Cover Image and the values of Stego Image. These differences are called residuals and the RMSE provide to combine them into a single measure of analytical power. The RMSE shows in (13):

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(X_{obs,i} - X_{model,i})^2}{n}} \quad (13)$$

$X_{obs,i}$ and $X_{model,i}$ are two image vectors i.e. cover and stego.

E. Structural Similarity Index (SSIM):

Wang et al. [47], proposed Structural Similarity Index concept between original and distorted image. The Stego and Cover images are divided into blocks of 8 x 8 and converted into vectors. Then two means and two standard derivations and one covariance value are computed.

After that the luminance, contrast and structure comparisons based on statistical values are computed. Then The SSIM [26] computed between Cover and Stego images. SSIM shows in (14).

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\mu_x^2 + \mu_y^2 + C_2)} \quad (14)$$

it has been observed that the SSIM values are nearest to 1, which shows that the cover and the stego both are prone to parallel and our human visual system can't recognize the changes occurred in the images.

F. K L Divergence (KLDIVG):

With the help of probability density function (PDF) for each Image (cover and stego) we estimate the Kullback-Leibler Divergence [48]. KL divergence shows in (15):

$$D(p\|q) = \sum_x p(x)\log\frac{p(x)}{q(x)} \quad (15)$$

G. Entropy:

Entropy is a measure of the uncertainty associated with a random variable [49]. Here, a 'message' means a specific

realization of the random variable. Equation (16) shows it.

$$\Delta S = \int \frac{dQ_{rev}}{T} \quad (16)$$

where, S is the entropy; T is the uniform thermodynamic temperature of a closed system divided into an incremental reversible transfer of heat into that system (dQ).

Here we have tested through some steganalysis technique because to access the security of the Steganography algorithm the attack is necessary. First exact detector of LSB replacement was the heuristic RS analysis [50. Then Sample Pairs (SP) analysis was analyzed and reformulated by Dumitrescu et al. [51] in 2002. In this work all the stego image is generated by the help of our algorithm and tested through steganalysis attack algorithm i.e. RS analysis. Fig. 15 shows the Analysis of attack of an RGB image (anu.jpg is used here) as cover and stego image. With the help of RS Analysis, we observe that, a typical images $R_{COVER} \approx R_{STEGO}$ and $S_{COVER} \approx S_{STEGO}$ and so no changes found in R and S value for embedding characters of different sizes.

VI. Comparison

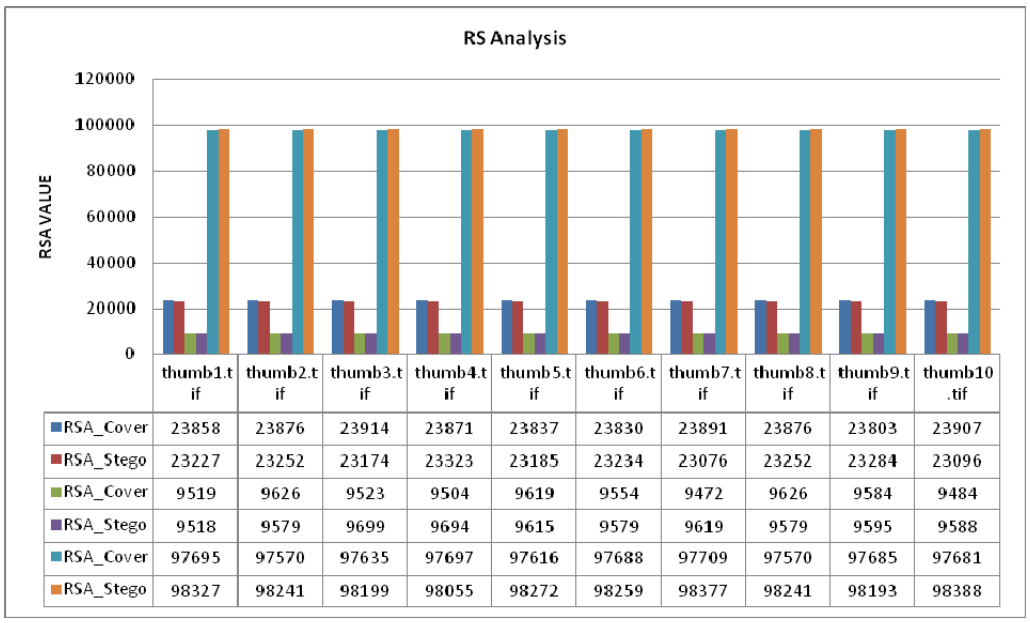
The comparison with other methods belongs to special as well as frequency domains are furnished below.

TABLE I
COMPARISON WITH OTHER SPATIAL DOMAIN STEGANOGRAPHIC METHOD

Other Methods [53], [54])	**This Method**
There is no embedding space determining concept per pixel.	Embedding space is determined per pixel by using a series of squared integers. **(α_{ij} and β_{ij})**
Message image is embedded directly.	Message image is not embedded directly but a polynomial $\sum^n$ is used which divides different length bit streams into different classes depending upon the value of k.
Embedding space does not vary from pixel to pixel.	Embedding space varies from pixel to pixel so that it may happen that no embedding is done for a pixel which ensures its security.
Stop bit is needed to denote the end of embedding.	Stop bit concept is not introduced here so that there are no such pixels which have different value form the other pixels which can be recognized easily.
For most of the methods one bit binary data is embedded.	0 or 1 or 2 or 3 or 4 bits of the message bit stream is embedded per pixel and if there is no sufficient embedding space for a plane then embedding is perform for the next plane.

TABLE II
COMPARISON WITH OTHER FREQUENCY DOMAIN BIOMETRIC STEGANOGRAPHIC METHOD

Others Methods [52]	**This Method**
Frequency domain has used.	Spatial domain is using, but it can work on frequency domain also.
Direct message embedding has been used.	Direct message is not embedding here.
Variable length cannot be supported by this method.	Variable length has been supported by this method.



	thumb1.tif	thumb2.tif	thumb3.tif	thumb4.tif	thumb5.tif	thumb6.tif	thumb7.tif	thumb8.tif	thumb9.tif	thumb10.tif
RSA_Cover	23858	23876	23914	23871	23837	23830	23891	23876	23803	23907
RSA_Stego	23227	23252	23174	23323	23185	23234	23076	23252	23284	23096
RSA_Cover	9519	9626	9523	9504	9619	9554	9472	9626	9584	9484
RSA_Stego	9518	9579	9699	9694	9615	9579	9619	9579	9595	9588
RSA_Cover	97695	97570	97635	97697	97616	97688	97709	97570	97685	97681
RSA_Stego	98327	98241	98199	98055	98272	98259	98377	98241	98193	98388

Fig. 15 RS Analysis for various Secret Images

VII. Conclusions

In this technique an image steganography process has been occurs by using a series for embedding space selection and a polynomial has been used for embedding the secret message, so that secret message bit is not embedded directly and makes difficult for steganalysis. Also for pixel selection mechanism,

the biometric features has been used which comes from both the cover and secret embedding information. From the security aspects the attack technique is very low between the cover image and stego image which have already surrender a very high security value of the hidden data. The hidden message also keeps on undetected after appliance of some renowned steganalysis method on it. In future we have planned to apply this technique in frequency domain for better security and furthermore outspread the practice in video domain.

REFERENCES

[1] Eskicioglu, A.M.; Litwin, L."Cryptography", Potentials, IEEE (Volume: 20, Issue:1), Feb/Mar 2001, Page(s): 36 - 38, ISSN : 0278-6648.
[2] Fu-Hau Hsu, Min-Hao Wu, Shiuh-Jeng WANG, "Dual-watermarking by QR-code Applications in Image Processing", 2012 9thInternational Conference on Ubiquitous Intelligence and Computing.
[3] Kaminsky, A. ; Kurdziel, M. ; Radziszowski, S."An overview of cryptanalysis research for the advanced encryption standard", Military Communications Conference, 2010 - MILCOM 2010,San Jose, CA , Oct.31 2010-Nov.3 2010, Page(s): 1310 - 1316, ISSN : 2155-7578
[4] Wenjun Zeng ; Liu, B."A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images" Image Processing, IEEE Transactions on (Volume:8 ,Issue: 11), Nov 1999, Page(s):1534 - 1548, ISSN : 1057-7149.
[5] N.N. EL-Emam, "Hiding a large amount of data with high security using steganography algorithm," Journal of Computer Science, vol. 3, no. 4, pp.223-232, April 2007.
[6] Krista Bennett (2004). "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text". CERIAS TR 2004-13.
[7] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal, "An Approach of Quantum Steganography through Special SSCE Code", International Journal of Computer and Information Engineering (WASET), Vol:5, No:8, Year:2011.
[8] V.Sathyal, K.Balasuhramaniyam, N.Murali, M.Rajakumaran, Vigneswari, "Data Hiding In Audio Signal, Video Signal Text And Jpeg Images", IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM-2012)March 2012. 741-746.
[9] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal, "A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier", Journal of Global Research in Computer Science(JGRCS), Volume 2, No. 4, April 2011.
[10] Souvik Bhattacharyya and Gautam Sanyal, "A Data Hiding Model with High Security Features Combining Finite State Machines and PMM method" International Journal of Computer and Information Engineering (WASET), Vol:4, No:8, Year:2010.
[11] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal. "Hiding & Analyzing Data in Image Using Extended PMM". In Proceedings of Computational Intelligence: Modeling, Techniques and Applications (CIMTA- 2013), Kalyani University, Kalyani, West Bengal, India, September 27-28, 2013. Proceedings published in "Procedia Technology, Elsevier".
[12] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal, "Study and Analysis of Steganography with Pixel Factor Mapping (PFM) Method", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 8, August 2013.
[13] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal, "Robust image steganography with pixel factor mapping (PFM) technique", Computing for Sustainable Global Development (INDIACom), 2014 International Conference on 5-7 March 2014. Page(s): 692 - 698, Print ISBN: 978-93-80544-10-6. Publisher: IEEE Xplore Digital Library.
[14] Jain.A.K, Hong.L, Pankanti.S: Biometric identification. Communications of the ACM 43 (2000) P. 91-98.
[15] A. K. Jain, A. Ross and S. Pankanti, Biometrics: A tool for information security, IEEE Transactions on Information Forensics and Security, vol.1, no.2, pp.125-143, 2006.
[16] K. A. Rhodes, Information Security: Challenges in Using Biometrics, United States General Accounting Office, 2003.
[17] A. K. Jain, A. Ross and S. Prabhakar, An introduction to biometric recognition, IEEE Transactions on Circuits and Systems for Video Technology, vol.14, no.1, pp.4-20, 2004.
[18] S. Prabhakar, S. Pankanti and A. K. Jain, Biometric recognition: Security and privacy concerns, IEEE Security and Privacy, vol.1, no.2, pp.33-42, 2003.
[19] A. K. Jain and A. Kumar, Biometrics of next generation: An overview, The 2nd Generation Biometrics, 2010.
[20] Y.K.Lee. & L.H.Chen."High capacity image steganographic model". IEEE Proc.-Vision, Image and Signal Processing,147:288–294, 2000.
[21] D.C. Wu. and W.H. Tsai. "A steganographic method for images by pixel value differencing". Pattern Recognition Letters, 24:1613–1626, 2003.
[22] P Huang. K.C. Chang., C.P Chang and T.M Tu. "A novel image steganography method using tri-way pixel value differencing". Journal of Multimedia, 3, 2008.
[23] Potdar V.and Chang E. "Gray level modification steganography for secret communication". In IEEE International Conference on Industria Informatics., pages 355–368, Berlin, Germany, 2004.
[24] Wien Hong and Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching." IEEE Transactions on Information Forensics And Security, Vol.7, No.1, Feb 2012, 176-184.
[25] Osman, H.;Mahjoup, W. ; Nabih, A. ; Aly, G.M. "JPEG encoder for low-cost FPGAs" Published in Computer Engineering & Systems, 2007. ICCES '07. International Conference on 27-29 Nov. 2007.
[26] Kobayashi, H., Y. Noguchi and H. Kiya (1999). "A method of embedding binary data into JPEG bitstreams". IEICE Trans. Information and Systems, J83-D-II, 1469–1476.
[27] N. Provos and P. Honeyman "Hide and seek: An introduction to steganography," IEEE Security and Privacy, vol. 1, no. 3, pp. 32-43, 2003.
[28] M. Titchener, "Technical note: Digital encoding by way of new T-codes," IEE Proceedings - Computers and Digital Techniques, vol. 131, no. 4, pp. 151-153, 1984.
[29] K. B. Raja, Vikas, Venugopal K. R and L. M. Patnaik, "High Capacity Lossless Secure Image Steganography using Wavelets,"International Conference on Advances Computing and Communications, pp. 230 – 235, 2006.
[30] Radovan Ridzon, Dushan Levisky and Tomas Kanocz, "Information Hiding within Still Images Based on the DCT Coefficients Flipping and Encryption," 52nd International Symposium, pp.147–150, September 2010.
[31] Chang, C.C., T.S. Chen and L.Z. Chung (2002). "A steganographic method based upon JPEG and quantization table modification". Information Sciences, 141, 123–138.
[32] J. Pedraza, M. A. Patricio, A. de Asís, and J. M. Molina, "Privacy and legal requirements for developing biometric identification software in context-based applications," International Journal of Bio-Science and Bio-Technology, vol. 2, no. 1, pp. 13–24, 2010.
[33] Subhra Mazumdar; Venkata Dhulipala. "Biometric Security Using Finger Print Recognition". University of California, San Diego. p. 3. Retrieved 30 August 2010.
[34] Retina and Iris Scans. Encyclopedia of Espionage, Intelligence, and Security. Copyright © 2004 by The Gale Group, Inc.
[35] R. Brunelli, Template Matching Techniques in Computer Vision: Theory and Practice, Wiley, ISBN 978-0-470-51706-2, 2009.
[36] Miroslav Bača; Petra Grd and Tomislav Fotak (2012). "4: Basic Principles and Trends in Hand Geometry and Hand Shape Biometrics". New Trends and Developments in Biometrics. InTech. Retrieved 1st December 2013.
[37] Shangling Song; Kazuhiko Ohnuma; Zhi Liu; Liangmo Mei; Akira Kawada; Tomoyuki Monma "Novel biometrics based on nose pore recognition" 2009.
[38] Surya Prakash, Umarani Jayaraman & Phalguni Gupta, A Skin-Color and Template Based Technique for Automatic Ear Detection, Proceedings of 7th International Conference on Advances in Pattern Recognition (ICAPR 2009), pp. 213-216, Kolkata, India, February 2009.
[39] Yeung, D; H., Xiong, Y., George, S., Kashi, R., Matsumoto, T., Rigoll, G; "SVC2004: First international signature verification competition". Lecture Notes in Computer Science. LNCS-3072: 16–22. 2004.
[40] Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons." Proceedings of the IEEE, vol. 94 (11), 2006, pp. 1927-1935.
[41] Homayoon Beigi, Speaker Recognition, Biometrics / Book 1, Jucheng Yang (ed.), Intech Open Access Publisher, 2011, pp. 3-28, ISBN 978-953-307-618-8.

[42] Wang, L.-Y., G. Leedham, and D. S.-Y. Cho, Infrared Imaging of Hand Vein Patterns for Biometric Purposes, The Institution of Engineering and Technology, Computer Vision, Vol. 1, pp. 113-122, 2007.
[43] Kumar, A., K. and K., V. Prathyusha, Personal authentication using hand vein triangulation, IEEE Trans. Image Process., Vol. 38, pp. 2127-2136, 2009.
[44] Yusra A. Y. Al-Najjar, Dr. Der Chen Soong, "Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI", International Journal of Scientific & Engineering Research, Volume 3, Issue 8, August-2012 ISSN 2229-5518
[45] Guillermito(2004).“Steganography: a few tools to discover hidden data”. Retrieved September, 2007, from http://www.guillermito2.net/stegano/tools/index.html
[46] J.L.Rodgers, J.L. and W.A.Nicewander, "Thirteen Ways to Look at the Correlation Coefficient", American Statistician 42, 59-66 (1995).
[47] Lehmann, E. L.; Casella, George (1998). “Theory of Point Estimation (2nd ed.)”. New York: Springer. ISBN 0-387-98502-6.
[48] Pedro J. Moreno, Purdy Ho, Nuno Vasconcelos "A Kullback-Leibler Divergence Based Kernel for SVM Classification in Multimedia Applications" Conference: Neural Information Processing Systems - NIPS , 2003
[49] Claude E. Shannon, "A mathematical theory of communication", The Bell System Technical Journal., 27:379–423.
[50] Patricia R. Pereira. Andr R.S. Maral. “A steganographic method for digital images robust to rs steganalysis”. Springer Lecture Notes in Computer Science, Vol. 3656., pages 1192–1199, 2005.
[51] S. Dumitrescu, X. Wu, and N. D. Memon. “On steganalysis of random LSB embedding in continuous-tone images”. In Proceedings IEEE, International Conference on Image Processing, ICIP 2002, pages 324–339, Rochester, NY, September 22–25, 2002.
[52] Amritha.G, Meethu Verkey. “Biometric Steganographic Technique Using DWT and Encryption” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, ISSN: 2277 128X.
[53] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta. “Hash Based Least Significant Bit Technique for Video Steganography”. International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012.
[54] Gabriel Macharia Kamau, Stephen Kimani, Waweru Mwangi. “An enhanced Least Significant Bit Steganographic Method for Information Hiding”. Journal of Information Engineering and Applications www.iiste.org ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol 2, No.9, 2012.

Souvik Bhattacharyya received his B.E. degree in Computer Science and Technology from B.E. College, Shibpur, India and M.Tech degree in Computer Science and Engineering from National Institute of Technology, Durgapur, India. He has received Ph.D (Engg.) from National Institute of Technology, Durgapur, India. Currently he is working as an Assistant Professor and In-Charge in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. His areas of interest are Natural Language Processing, Network Security and Image Processing. He has published nearly 70 papers in International and National Journals / Conferences

Indradip Banerjee is a Research Scholar at National Institute of Technology, Durgapur, West Bengal, India. He received his MCA degree from IGNOU in 2009, PGDCA from IGNOU in 2008, MMM from Annamalai University in 2005 and BCA (Hons.) from The University of Burdwan in 2003. He is registered and pursuing his PhD in Engineering at Computer Science and Engineering Department, National Institute of Technology, Durgapur, West Bengal, India. His areas of interest are Biometric Information Security, Steganography, Cryptography, Text Steganography, Image Steganography, Quantum Steganography and Steganalysis. He has published 22 research papers in International and National Journals / Conferences.

Anumoy Chakborty received his MCA degree from Vidyasagar University and currently doing his M.E in Computer Science and Engineering from University Institute of Technology, The University of Burdwan. He is a final year student of this course and his areas of interest are Database, Web Technology, Biometric Information Security, Network Security and Computer Network.

Gautam Sanyal has received his B.E and M.Tech degree National Institute of Technology (NIT), Durgapur, India. He has received Ph.D (Engg.) from Jadavpur University, Kolkata, India, in the area of Robot Vision. He possesses an experience of more than 25 years in the field of teaching and research. He has published nearly 150 papers in International and National Journals / Conferences. Two Ph.Ds (Engg) have already been awarded under his guidance. At present he is guiding six Ph.Ds scholars in the field of Steganography, Cellular Network, High Performance Computing and Computer Vision. He has guided over 10 PG and 100 UG thesis. His research interests include Natural Language Processing, Stochastic modeling of network traffic, High Performance Computing, Computer Vision. He is presently working as a Professor in the department of Computer Science and Engineering and also holding the post of Dean (Students’ Welfare) at National Institute of Technology, Durgapur, India.