iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3463

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Robust Variable Embedding Retinal Biometric Steganography and Authentication Checking

Pabak Indu[1], Souvik Bhattachryya [2]
[1] *School of Computers, Inspiria Knowledge Campus, Siliguri, West Bengal, India*
[2]*Department of Computer Science and Engineering, University Institute of Technology, The University of Burdwan, Burdwan, India*

Abstract*: *Attacks, misuse or unauthorized access of information is of great concern today, which makes the protection of documents through digital media a priority problem. The Biometric Steganography plays a vital role in maintaining the secrecy of the secret information in today's world of communication. Although the biometric system along is always at the risk of suffering the possibility of different types of attacks. The super imposition of biometric system in steganography principle has drastically cuts down those potential risks. This paper has proposed a new approach of information hiding methodology in the area of retinal biometric steganography in combination with biometric authentication principle. Experimental results demonstrate the effectiveness and accuracy of the proposed methodology in terms of security of hidden data with maintaining the integrity and authentically of it.

Keywords*: *Authentication checking, Retinal Biometric Steganography, Pixel Selection, Feature Extraction, Polynomial value digation.

I. INTRODUCTION

In current digitized world humane race is facing a great revolution over Internet Technologies where every single information needs to be transmitted securely through some communication media.

This results the birth of different Information Hiding methodologies like, Steganography, Cryptography, Watermarking etc. [1]. The first two techniques provide protection on data whereas the third one gives the authentication of data. Steganography is an area of information hiding which means "secret or covered writing". Almost all digital file formats can be used for steganography, but the image and audio files are more suitable because of their high degree of redundancy [2].

Biometric security system is an automatic recognition system of an individual through the aid of the physiological and behavioural [3]–[7] characteristic. The term "biometrics" is a Greek word where the word "bio" means "life" and "metric" means "to measure". This system finds out the person's uniqueness based on pattern analyses, carried out on unambiguous human behaviour [4], [5]. Physiological biometric systems consist of fingerprints, retina, iris, hand geometry, hand vein, ear shape and facial recognition systems [6] where the features are usually unalterably processed by human being.

In the contrary, the behavioural biometric characteristics are valid over a short span of time. Examples of behavioral biometric systems are voice recognition, keystroke dynamics, signature verification and gait analysis [7]. Biometrics refers to the automatic identification of a person based on his or her physiological or behavioural characteristics.

This identification method is preferred over traditional methods involving passwords and personal identification numbers (PINs). Uses of biometric techniques has been gaining popularity day-by –day due its features like Uniqueness, Universality, Performance, Measurability and User friendliness.

In this work a specific image based biometric steganography method has been proposed which may be considered as the improved version of the author's previous work [8] with an additional approach of authentication of the secret message, key or password embeds into transform domain portions of cover image with the help of the biometric features. This developed contribution is a novel biometric steganography technique, where the secret message hiding is done in the Transform domain with variable length embedding technique as a bit stream of two to four bits combinations and authentication checking is done in the spatial domain of the same image with the aid of some biometric retinal features.

Rest of the paper has been organized as following sections: Section II describes some associated works on image steganography. Section III deals with proposed method. Section IV and V has been used for describing the Algorithms and Mathematical Analysis of the proposed system respectively. In section VI experimental results has been discussed and finally section VII draws the conclusion.

II. RELATED WORK

In this section some image based steganography data hiding methods in both spatial domain and transform domain has been discussed. This section also discusses some existing Biometric Security Techniques.

A. *Image Steganography Techniques:*

The image steganography can be designed and implemented in two domains, one is Spatial and another one is in transform domain. There are numerous approaches exists in both domains. Some of them are discussed below:

1) *Spatial Domain Technique:* The most common technique in this domain is data hiding by least-significant-bit (LSB) [9] which works based on manipulating the least-significant bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. The pixel-value differencing (PVD) method proposed by Wu and Tsai [10] can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image. In 2004, Potdar et al. [11] proposes GLM (Gray level modification) technique which is used to map data by modifying the gray level of the image pixels. Hong and Chen [12] introduced a new method based on pixel pair matching (PPM). Bhattacharyya and Sanyal proposed a new image transformation technique known as Pixel Mapping Method (PMM) [13], [14] a method for information hiding within the spatial domain of any gray scale image. 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. Banerjee et al. [15] proposes Pixel Factor Mapping (PFM) technique which embeds the four bits of secret message in a single pixel intensity based on the maximum prime factor value of pixel intensity.
2) *Transform Domain Technique:* Transform domain steganography method hides messages in significant areas of cover image which makes them robust against various image processing operations like compression, enhancement etc. The widely used transformation functions include Discrete Cosine Transformation (DCT), Discrete Fourier Transform (DFT), and Wavelet Transformation.
3) *DCT based Data Hiding:* J-Steg [16] and JP Hide [17] are the two classical JPEG steganography tools developed based on LSB embedding technique. F5 steganography algorithm was introduced by West feld [18] where instead of replacing the LSBs of quantized DCT coefficients with the message bits, it modifies the randomly-chosen coefficient by decreasing the absolute value of the coefficient by one. Out Guess [19] has been developed through UNIX. Yet Another Steganography Scheme (YASS) [20] works based on the principle of JPEG steganography but does not directly embed data in JPEG DCT coefficients. Instead an input image in spatial domain is divided into blocks with a fixed large size known as the big blocks (or B-blocks). MB steganography methods has been proposed for JPEG images, achieves a high embedding efficiency and message capacity than the previous methods also remains secure against first order statistical attacks. BCH and BCHopt [21] are side-informed algorithms that employ BCH codes to minimize the embedding distortion in the DCT domain defined using the knowledge of non-rounded DCT coefficients. Wang et al. [22] presents an efficient JPEG steganography scheme based on the block entropy of DCT coefficients and syndrome trellis coding (STC). Bhattacharyya et al. [23]introduced DCTDM, which can embed via modulating adjacent DCT coefficient differences.
2 *DWT based Data Hiding:* Wavelet-based steganography [24] and [25] is a new idea in the application of wavelets. However, the standard technique of storing in the least significant bits (LSB) of a pixel still applies. The only difference is that the information is stored in the wavelet coefficients of an image, instead of changing bits of the actual pixels.

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 [26]. In biometric technique there are various ways and all biometric techniques differ according to security level, user acceptance, cost and performance. Fig. 1 describes the classification of biometric techniques.

222Fingerprints: Fingerprint [27] is one of the techniques which provide biometric securities, based on fingertip pattern recognition. There are three basic patterns of fingerprint ridges: i) Arch: Ridges enter from one side of the finger, forming in the center and exit the other side of the finger. ii) Loop: Ridges enter from one side of a finger then form a curve and then exit on that same side. iii) Whorl: The ridges form circularly around a central point on the finger.

1) *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 [28].
2) *Face:* Face biometry [29] depends on analyzing facial characteristics. It is automatically identifying or verifying a person from an image.

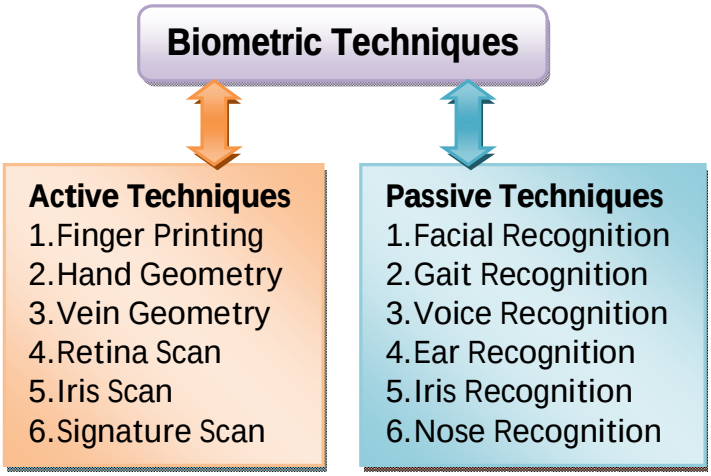


Fig 1: Classification of biometric techniques

3) *Hand Geometry:* In this mechanism [30] the shape of the human hand is computed and analyzed 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.
4) *Nose:* The nose biometric technique [31] works through features extracting from a nose and by the help of various classification techniques.
5) *Ear:* One of interesting authentication technique is ear biometric security. Analyzing ear shape and area measurement of a human can be identified easily [32]
6) *Signature:* 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 [33]. It can be operated in two different ways like Static and Dynamic
7) *Iris:* In this iris-based biometric system [34] features are analyzed using mathematical pattern-recognition techniques. It stores the measurement of the colored ring of tissue surrounds the pupil of eye.
8) *Voice:* Voice biometrics [35] has the most probable for enlargement, because it requires no new hardware, most PCs have already contained a microphone.
9) *Vein geometry:* In this technique the vein of hand, vein of finger, vein of palm etc. are used for authentication purpose. L. Wang et al. [36] proposed a verification system of human beings using the thermal-imaged vein pattern in the back of hand. A. Kumar et al. [37] presents a technique which can authenticate a person based on minutiae matching of vein junction points.
10) *Face geometry:* One of the physiological characteristics is Face geometry [38] for recognition of a human. The relative location of human face objects like mouth, eye, nose etc in the face is unique for each human being. Face length, height, width, curvatures, relative location like distance and angles of facial objects has been observed in the face geometry of a human face.

III.PROPOSED METHOD

In this work a new approach of biometric steganography technique has been proposed which works in a combined approach like transform and spatial domain in a same image. This biometric steganography technique has been designed for embedding secret message in the skin tone portion of the human face using variable length message embedding algorithm in transform domain with the help of discrete cosine transform and biometric features of retinal images like Rod and Cone count for authenticity checking, in spatial domain. The block diagram of the proposed system has been shown in Fig. 2. The system first performs biometric features embedding in spatial domain then performs embedding in transform domain which divides the system architecture in two parts

A. Biometric Features Embedding in Spatial Domain

This architecture consists of the steps as depicted in fig. 2 and block diagram of each steps are given below.

1) *Step1: Load Cover Image* – In this step the cover image is loaded into the system and border cells are cropped.

2) *Step2: Skin Tone Detection* – In this step the skin tone area detection in the input cover image is performed by setting some threshold value on hue plane and saturation plane of HSV color space.

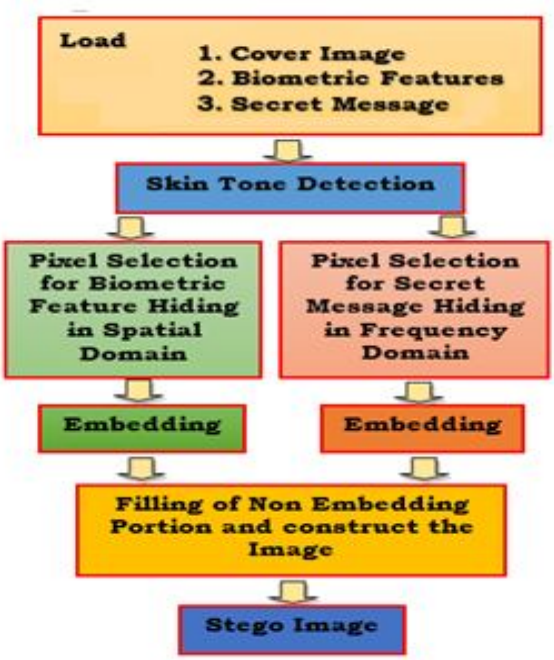


Fig 2: Block Diagram of Proposed System

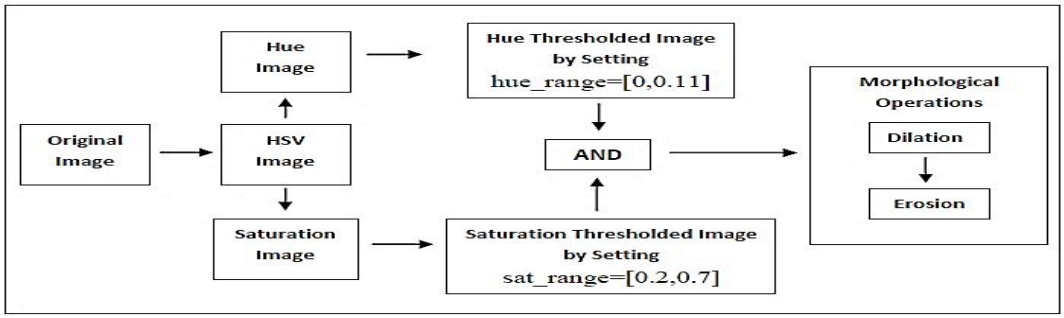


Fig 3: Block Diagram of Skin Tone Detection

3) *Step3: Pixel Selection for Biometric feature embedding in Spatial Domain* – In this step the system select those pixels for spatial domain embedding out of pixels selected through skin tone detection by dividing the whole image in 5 X 5 blocks and selecting pixels on every first row and first column of each block only on skin tone detected area.

In this work the skin region of the image has been used for embedding of secret data as well as biometric features. The system detects the skin color with the help of skin detector and skin classifier. Skin detector has been used to convert the RGB color space into appropriate color space HSV, as because it is more appropriate for human colour perception. For skin detection threshold value has been chosen for Hue as well as Saturation range. Next skin classifier classifies the pixels of 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.

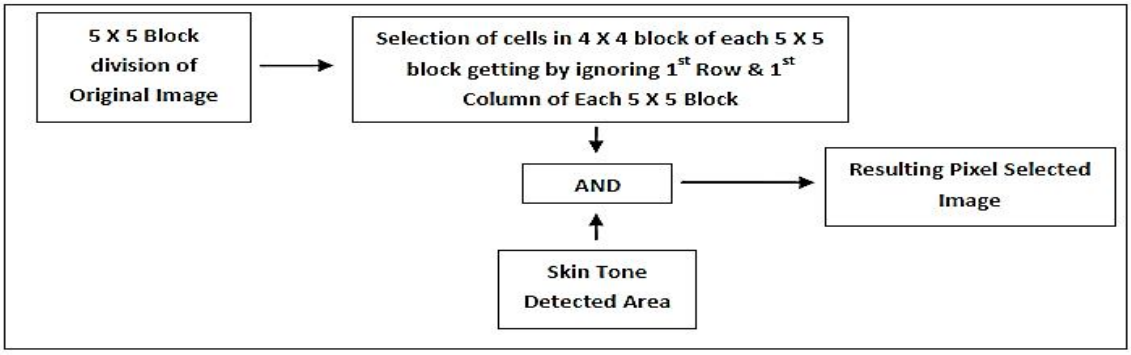


Fig 4: Block Diagram of Pixel Selection for Biometric Feature Embedding in Spatial Domain

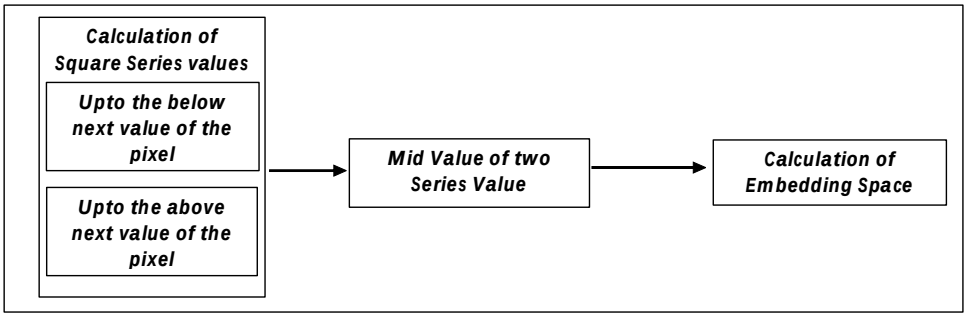
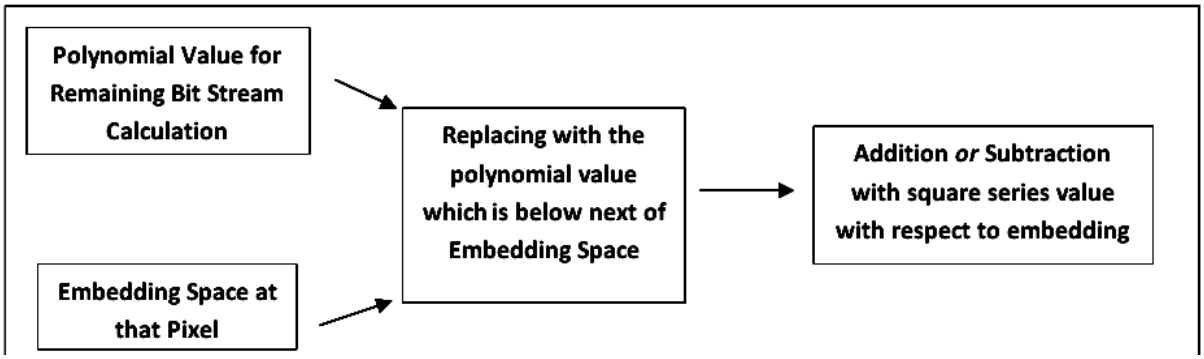


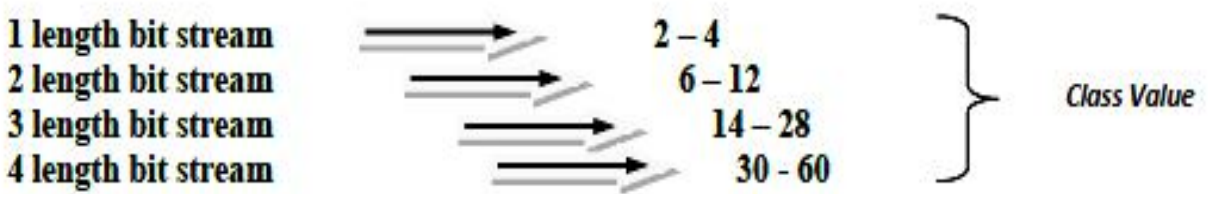
Fig 5: Block Diagram of Embedding Pixel Selection

4) *Step4: Embedding Pixel Selection* –Pixel for embedding space has been selected with the help of two square series having above next and below next value of the concern pixel value. In the next step it calculates the mid value of those two square series. If the resulting mid value is greater than the pixel value then embedding pixel value is calculated by subtracting the concern pixel value from the below next square series value of the pixel. Else if the resulting mid value is lower than the concern pixel value then embedding pixel value is calculated by subtracting the concern pixel value from the above next square series value of the pixel.
5) *Step5: Embedding through variable bit length* – Based upon the availability of embedding space the message bit stream is embedded in the resulting polynomial value format.

The embedding polynomial used here is as follows:

$\sum n=(xn.(k+bit_1))+(\lambda xn\text{-}1.(k+bit_2))+(xn\text{-}2.(k+bit_3))$ +.....+$(x.(k+bit_n))$,where, $bit_n=n^{th}$ bit of remainder bit stream and k be a value which classify the polynomial value for different length bit stream. Thus for different k values the polynomial generates different class values for different length bit stream in the following manner.





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 particular plane then the system perform embedding in next plane. Table I below explain the embedding principle for k=1.

TABLE I
WORKING PRINCIPLE OF EMBEDDING POLYNOMIAL IN SPATIAL DOMAIN

Bit Stream	*Polynomial*	*Polynomial Value*
0	$2(1+0)$	2
1	$2(1+1)$	4
00	$2^2(1+0)+2(1+0)$	6
01	$2^2(1+0)+2(1+1)$	8
10	$2^2(1+1)+2(1+0)$	10
11	$2^2(1+1)+2(1+1)$	12
000	$2^3(1+0)+2^2(1+0)+2(1+0)$	14
001	$2^3(1+0)+2^2(1+0)+2(1+1)$	16
010	$2^3(1+0)+2^2(1+1)+2(1+0)$	18
011	$2^3(1+0)+2^2(1+1)+2(1+1)$	20
100	$2^3(1+1)+2^2(1+0)+2(1+0)$	22
101	$2^3(1+1)+2^2(1+0)+2(1+1)$	24
110	$2^3(1+1)+2^2(1+1)+2(1+0)$	26
111	$2^3(1+1)+2^2(1+1)+2(1+1)$	28
0000	$2^4(1+0)+2^3(1+0)+2^2(1+0)+2(1+0)$	30
0001	$2^4(1+0)+2^3(1+0)+2^2(1+0)+2(1+1)$	32
0010	$2^4(1+0)+2^3(1+0)+2^2(1+1)+2(1+0)$	34
0011	$2^4(1+0)+2^3(1+0)+2^2(1+1)+2(1+1)$	36
0100	$2^4(1+0)+2^3(1+1)+2^2(1+0)+2(1+0)$	38
0101	$2^4(1+0)+2^3(1+1)+2^2(1+0)+2(1+1)$	40
0110	$2^4(1+0)+2^3(1+1)+2^2(1+1)+2(1+0)$	42
0111	$2^4(1+0)+2^3(1+1)+2^2(1+1)+2(1+1)$	44
1000	$2^4(1+1)+2^3(1+0)+2^2(1+0)+2(1+0)$	46
1001	$2^4(1+1)+2^3(1+0)+2^2(1+0)+2(1+1)$	48
1010	$2^4(1+1)+2^3(1+0)+2^2(1+1)+2(1+0)$	50
1011	$2^4(1+1)+2^3(1+0)+2^2(1+1)+2(1+1)$	52
1100	$2^4(1+1)+2^3(1+1)+2^2(1+0)+2(1+0)$	54
1101	$2^4(1+1)+2^3(1+1)+2^2(1+0)+2(1+1)$	56
1110	$2^4(1+1)+2^3(1+1)+2^2(1+1)+2(1+0)$	58
1111	$2^4(1+1)+2^3(1+1)+2^2(1+1)+2(1+1)$	60

6) Step6: Filling up Non Embedding Portions : Remaining non embedding portions is filled by the system with respect to the selected square series value of that pixel. Since the embedding polynomial value is always even number for spatial domain thus if the selected square series value is odd number then the pixel value is made to an even number for denoting that no data has been embedded there.

7) Step7: Stego Image Creation –Resulting Stego image for Spatial Domain is created.

B. Secret Message Hiding in Transform Domain:

The architecture consists of the steps which is depicted in below figures.

1) *Step1: Load Cover Image* – In this step the cover image is loaded into the system and border cells are cropped.
2) *Step2: Skin Tone Detection* – Already explained earlier.
3) *Step3: Pixel Selection for Secret Message Hiding in Transform Domain* – For hiding secret message in Transform domain, the procedure made a block processing on the resulting cropped image which is cropped into 5 X 5 blocks and take the 4 X 4 block of each 5 X 5 blocks by ignoring first row and first column, since spatial domain embedding operation is performed at those cells contained in first row and first column.

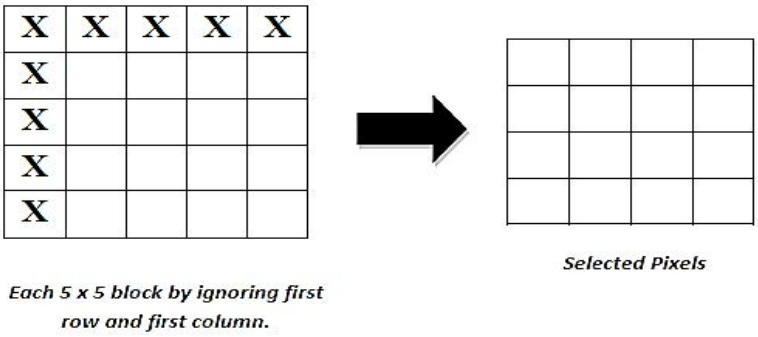


Fig 7: Pixel Selection on each block

4) *Step4: Preprocessing for Embedding* – This steps performs two dimensional Discrete Cosine Transformation (DCT2) on 4 X 4 block of each 5 X 5 block by ignoring 1st row and 1st column. Then the system ignore topmost left corner cell value and extract the integer part of other cell values of the 4 X 4 block.

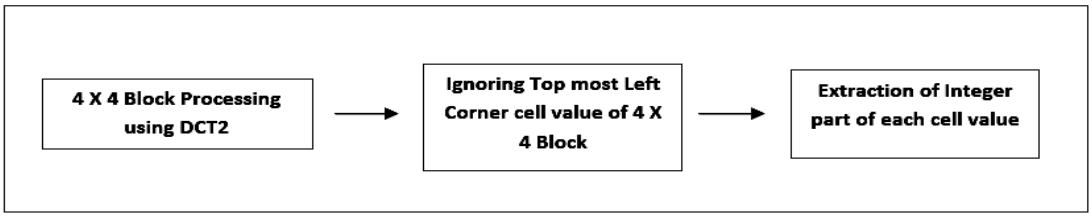


Fig 8: Block Diagram of Preprocessing

For hiding secret message in Transform domain it made a block processing on the resulting cropped image which divide the cropped image into 5 X 5 blocks and take the 4 X 4 block of each 5 X 5 blocks by ignoring first row and first column, since spatial domain embedding operation is performed at those cells contained in first row and first column.

998.2345	7.376	-20.98	100.287
34.67	-27.834	89.342	78.534
56.783	46.983	-29.345	55.439
12.678	0.534	29.356	78.243

0	7	20	100
34	27	89	78
56	46	29	55
12	0	29	78

Fig 9: Cell value extraction

5) *Step5: Embedding Space Selection* –As the technique the system follows embedding space varies from pixel to pixel. To get the embedding space of a cell of each block the system uses a series of integers and thus the system adds the squared value of integers up to the below next value α_{ij} of the cell value $Cell_{ij}$ and also do the same up to the next above value β_{ij} of the cell value $Cell_{ij}$. As for example, $Cell_{ij}$ =127.

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

Then the system calculate the mid value by $\gamma_{ij}=(\alpha_{ij}+ \beta_{ij})/2$ and if $Cell_{ij}$ is less than or equal to the mid value γ_{ij} then it get the subtracted value $\delta_{ij}=(Cell_{ij} - \alpha_{ij})$ else $\delta_{ij}=(\beta_{ij}- Cell_{ij})$ as embedding space. Thus after getting the embedding space for each cell $Cell_{ij}$ the system will further approach for embedding.

6) *Step5: Embedding* – With respect to the availability of embedding space the message bit stream is embedded in the resulting polynomial value format.

The embedding polynomial used here is as follows:

$\sum^{n}=x^n.(k+bit_1)+x^{n-1}.(k+bit_2)+x^{n-2}.(k+bit_3)+.....+x.(k+bit_n)$, where, $bit_n=n^{th}$ bit of remainder bit stream and *k* be a value which classify the polynomial value for different length bit stream. Thus for different *k* values the polynomial generates different class values for different length bit stream.

a) *Step 5.1: Choosing value of the parameters of the polynomial with respect to embedding in Transform domain* – In Transform domain the embedded message is changed to the interval [+2 -2] at the extraction time, so at extraction time it is difficult extract the original message and this problem is overcome here by choosing the parameter values of the polynomial in such a manner so that it produces values with difference of 5 between each consecutive values. So that at extraction time the system will fetch the nearest value of the polynomial. Thus the system makes two halves of each polynomial value up to the range +2 and -2.

As for example, if the polynomial value 10 is change to 10 – 2 =8, then the system will automatically choose the nearest value 10 as it knows that the highest change can occur in the interval [+2 -2].

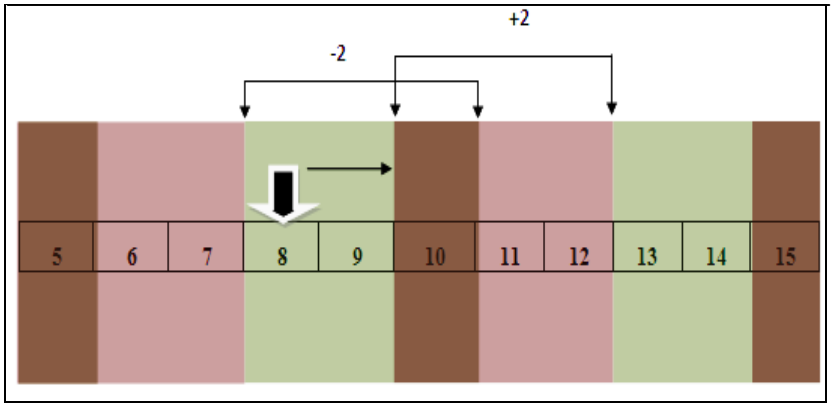


Fig 10: Value Fetching (Lower)

Similarly, if the polynomial value 10 is change to 10 + 1 =11 as the pointer point to in fig. 10 then the system will automatically choose the nearest value 10 as it knows that the highest change can occur in the interval [+2 -2].

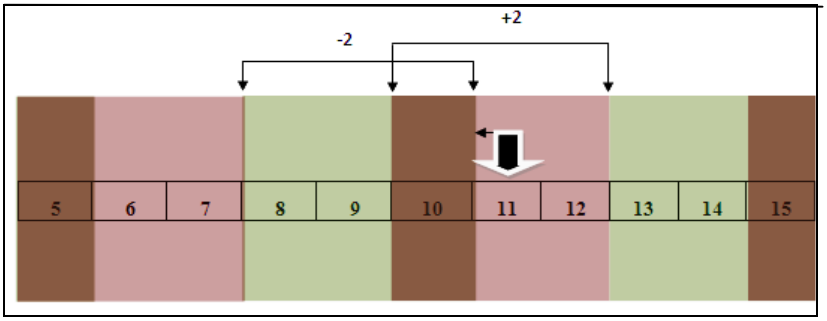


Fig 11: Value Fetching (Higher)

Table II below explain the embedding principle for x=5 and k=1.

TABLE II
WORKING PRINCIPLE OF EMBEDDING POLYNOMIAL IN TRANSFORM DOMAIN

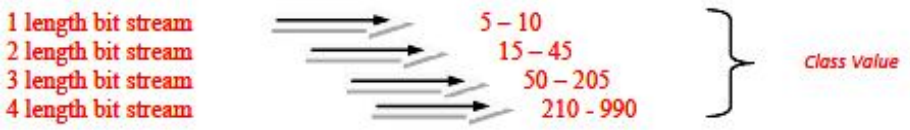
Bit Stream	Polynomial	Polynomial Value
0	$5(1+0)$	5
1	$5(1+1)$	10
00	$5^2(1+0)+5(1+0)$	30
01	$5^2(1+0)+5(1+1)$	35
10	$5^2(1+1)+5(1+0)$	55
11	$5^2(1+1)+5(1+1)$	60
000	$5^3(1+0)+5^2(1+0)+5(1+0)$	155
001	$5^3(1+0)+5^2(1+0)+5(1+1)$	160
010	$5^3(1+0)+5^2(1+1)+5(1+0)$	180
011	$5^3(1+0)+5^2(1+1)+5(1+1)$	185
100	$5^3(1+1)+5^2(1+0)+5(1+0)$	280
101	$5^3(1+1)+5^2(1+0)+5(1+1)$	285
110	$5^3(1+1)+5^2(1+1)+5(1+0)$	305
111	$5^3(1+1)+5^2(1+1)+5(1+1)$	310
0000	$5^4(1+0)+5^3(1+0)+5^2(1+0)+5(1+0)$	780
0001	$5^4(1+0)+5^3(1+0)+5^2(1+0)+5(1+1)$	785
0010	$5^4(1+0)+5^3(1+0)+5^2(1+1)+5(1+0)$	805
0011	$5^4(1+0)+5^3(1+0)+5^2(1+1)+5(1+1)$	810
0100	$5^4(1+0)+5^3(1+1)+5^2(1+0)+5(1+0)$	905
0101	$5^4(1+0)+5^3(1+1)+5^2(1+0)+5(1+1)$	910
0110	$5^4(1+0)+5^3(1+1)+5^2(1+1)+5(1+0)$	930
0111	$5^4(1+0)+5^3(1+1)+5^2(1+1)+5(1+1)$	935
1000	$5^4(1+1)+5^3(1+0)+5^2(1+0)+5(1+0)$	1405
1001	$5^4(1+1)+5^3(1+0)+5^2(1+0)+5(1+1)$	1410
1010	$5^4(1+1)+5^3(1+0)+5^2(1+1)+5(1+0)$	1430
1011	$5^4(1+1)+5^3(1+0)+5^2(1+1)+5(1+1)$	1435
1100	$5^4(1+1)+5^3(1+1)+5^2(1+0)+5(1+0)$	1530
1101	$5^4(1+1)+5^3(1+1)+5^2(1+0)+5(1+1)$	1535
1110	$5^4(1+1)+5^3(1+1)+5^2(1+1)+5(1+0)$	1555
1111	$5^4(1+1)+5^3(1+1)+5^2(1+1)+5(1+1)$	1560

b) *Step 5.2: Digestion of Polynomial Values:* To digest the polynomial values to the system for embedding so that maximum bit can embed another processing is done by the system that is digestion of polynomial values by subtracting 0 for 1 bit message value, 15 for two bit message value, 105 for three bit message value and 570 for four bit message value.

TABLE III
DIGESTION OF POLYNOMIAL VALUES OF TABLE II

Bit Stream	*Polynomial*	*Polynomial Value*	*Digestion*	*Digested Value*
0	$5(1+0)$	5	5-0	5
1	$5(1+1)$	10	10-0	10
00	$5^2(1+0)+5(1+0)$	30	30-15	15
01	$5^2(1+0)+5(1+1)$	35	35-15	20
10	$5^2(1+1)+5(1+0)$	55	55-15	40
11	$5^2(1+1)+5(1+1)$	60	60-15	45
000	$5^3(1+0)+5^2(1+0)+5(1+0)$	155	155-105	50
001	$5^3(1+0)+5^2(1+0)+5(1+1)$	160	160-105	55
010	$5^3(1+0)+5^2(1+1)+5(1+0)$	180	180-105	75
011	$5^3(1+0)+5^2(1+1)+5(1+1)$	185	185-105	80
100	$5^3(1+1)+5^2(1+0)+5(1+0)$	280	280-105	175
101	$5^3(1+1)+5^2(1+0)+5(1+1)$	285	285-105	180
110	$5^3(1+1)+5^2(1+1)+5(1+0)$	305	305-105	200
111	$5^3(1+1)+5^2(1+1)+5(1+1)$	310	310-105	205
0000	$5^4(1+0)+5^3(1+0)+5^2(1+0)+5(1+0)$	780	780-570	210
0001	$5^4(1+0)+5^3(1+0)+5^2(1+0)+5(1+1)$	785	785-570	215
0010	$5^4(1+0)+5^3(1+0)+5^2(1+1)+5(1+0)$	805	805-570	235
0011	$5^4(1+0)+5^3(1+0)+5^2(1+1)+5(1+1)$	810	810-570	240
0100	$5^4(1+0)+5^3(1+1)+5^2(1+0)+5(1+0)$	905	905-570	335
0101	$5^4(1+0)+5^3(1+1)+5^2(1+0)+5(1+1)$	910	910-570	340
0110	$5^4(1+0)+5^3(1+1)+5^2(1+1)+5(1+0)$	930	930-570	360
0111	$5^4(1+0)+5^3(1+1)+5^2(1+1)+5(1+1)$	935	935-570	365
1000	$5^4(1+1)+5^3(1+0)+5^2(1+0)+5(1+0)$	1405	1405-570	835
1001	$5^4(1+1)+5^3(1+0)+5^2(1+0)+5(1+1)$	1410	1410-570	840
1010	$5^4(1+1)+5^3(1+0)+5^2(1+1)+5(1+0)$	1430	1430-570	860
1011	$5^4(1+1)+5^3(1+0)+5^2(1+1)+5(1+1)$	1435	1435-570	865
1100	$5^4(1+1)+5^3(1+1)+5^2(1+0)+5(1+0)$	1530	1530-570	960
1101	$5^4(1+1)+5^3(1+1)+5^2(1+0)+5(1+1)$	1535	1535-570	965
1110	$5^4(1+1)+5^3(1+1)+5^2(1+1)+5(1+0)$	1555	1555-570	985
1111	$5^4(1+1)+5^3(1+1)+5^2(1+1)+5(1+1)$	1560	1560-570	990

Thus for different k values the polynomial generate different class values for different length bit stream. For x=5 and k=1 different class values are given below



Here the class values will vary for different value of k.

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.

C. Final Stego Image Creation

Final stego image is created by merging Spatial Domain Stego image and Transform Domain Stego image and incorporating the border cells achieved at Step 1.

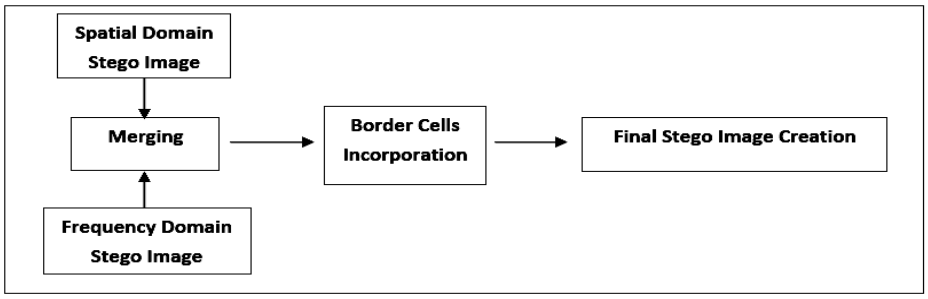


Fig 12: Block Diagram of Final Stego Image Creation

D. Feature Extraction from retina Image

Retinal Recognition of a person is done by acquiring an internal body image, the retinaof a person. Unlike other biometric technologies retinal recognition is not widely deployed in commercial applications .n while considered invasive and expensive, retinal recognition is still themostreliable and stable means of biometric identification. Although the advantages of retinal recognition currently outweigh the disadvantages, its widespread use is held back by public acceptance. The retina is a thin layer of cells at the back of the eye ball of vertebrates. It is the part of the eye which converts light into nervous signals

The retina consists of multiple layers of sensoryt issue and millions of photoreceptors (cells) whose function is to transform light rays into neural impulses. These impulses subsequently travel to the brainvia the optic nerve, where they are converted to images. Two distinct types of photoreceptors exist within the retina: the rods and the cones. While the cones (6million per eye) help us to see different colors, the rods (125 million per eye) facilitate night and peripheral vision. It is the unique structure of the blood vessel pattern in the retina that forms the foundation for retinal recognition and has been used for biometric identification.

Structure of rods and cons: Rods sense to brain brightness, Cones sense color the retina, in the back of the eye. It has cells that are sensitive to light. They connect directly to your brain.

IV. MATHEMATICAL REPRESENTATION

A. Problem Formulation

The mathematical representation of the proposed method is described on embedding side and extraction side.

Let, I be a M X N matrix with each cell value $Cell_{ij}$.

Also, let us consider two series values $\alpha_{ij}$and β_{ij}

Such that $\alpha_{ij}=1^2+2^2+3^2+4^2+5^2+6^2+\ldots <Cell_{ij}$and $\beta_{ij}=1^2+2^2+3^2+4^2+5^2+6^2+7^2+\ldots >Cell_{ij}$

Then mid value, $\gamma_{ij}=(\alpha_{ij}+ \beta_{ij})/2$

if $Cell_{ij}<= \gamma_{ij}$ then $\delta_{ij}=(Cell_{ij} - \alpha_{ij})$ else $\delta_{ij}=(\beta_{ij}-Cell_{ij})$

Let us suppose that embedding value is Emb_{ij}

Such that $Emb_{ij}<\delta_{ij}$and Stego Value is S_{ij}

if $Cell_{ij}<= \gamma_{ij}$ then $S_{ij}=(\alpha_{ij}+ Emb_{ij})$

else $S_{ij} =(\beta_{ij}- Emb_{ij})$

The embedding polynomial used here is as follows-

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

Where, bit_n=n^{-th} bit of remainder bit stream and k= value which classify the polynomial value for different length bit stream.
On Extraction side, for each cell S_{ij} of matrix I :-
α_{ij}:= $1^2+2^2+3^2+4^2+5^2+6^2+\ldots$ <$Cell_{ij}$
β_{ij}:= $1^2+2^2+3^2+4^2+5^2+6^2+7^2+\ldots$ >$Cell_{ij}$
γ_{ij}:=(α_{ij}+ β_{ij})/2
if S_{ij}<= γ_{ij}thenδ_{ij}:=(S_{ij} - α_{ij}) else δ_{ij}:=(β_{ij}- S_{ij})

B. Proof of the Problem

Prove that the above formulation gives exact result on extraction side as it was embed on embedding side.
Proof. Let, I be a M X N matrix with each cell value $Cell_{ij}$.
On Embedding Side
Let us consider two series values $\alpha_{ij}$and β_{ij}
such that α_{ij}=$1^2+2^2+3^2+4^2+5^2+6^2+\ldots$ <$Cell_{ij}$ and β_{ij}=$1^2+2^2+3^2+4^2+5^2+6^2+7^2+\ldots$ >$Cell_{ij}$
Then mid value, γ_{ij}=(α_{ij}+ β_{ij})/2 …….. (1)
if $Cell_{ij}$<= γ_{ij} then δ_{ij}=($Cell_{ij}$ - α_{ij}) ……..(2)
else δ_{ij}=(β_{ij}-$Cell_{ij}$) ……(3)
Let us suppose that embedding value is Emb_{ij}
Such that Emb_{ij}<$\delta_{ij}$and Stego Value is S_{ij}
if $Cell_{ij}$<= γ_{ij} then S_{ij}=(α_{ij}+ Emb_{ij}) ……....(4)
else S_{ij} =(β_{ij}- Emb_{ij}) ……..……(5)
On Extraction Side
For each cell $Cell_{ij}$of matrix I :-
α_{ij}:= $1^2+2^2+3^2+4^2+5^2+6^2+\ldots$ <$Cell_{ij}$
β_{ij}:= $1^2+2^2+3^2+4^2+5^2+6^2+7^2+\ldots$ >$Cell_{ij}$
γ_{ij}:=(α_{ij}+ β_{ij})/2
if S_{ij}<= γ_{ij}then δ_{ij}:=(S_{ij} - α_{ij}) ……..……(6)
else δ_{ij}:=(β_{ij}- S_{ij})……..……(7)
Now, using equation (4) & (5) in (6) & (7) we have
if S_{ij}<= γ_{ij}then δ_{ij}=((α_{ij}+ Emb_{ij}) - α_{ij})
= Emb_{ij}……....(8)
else δ_{ij}=(β_{ij}-(β_{ij}- Emb_{ij}))
= Emb_{ij}……..(9)
Since we embed the value in δ_{ij}on embedding side and from equation (8) & (9) we get δ_{ij}= Emb_{ij}. Hence it is proved.

V. ALGORITHMS

In this section various algorithm for data hiding in transform domain and biometric features embedding for authentication checking has been described.

A. Pixel Selection Algorithm by Skin Tone Detection

1) Read : cover image
2) Convert : cover image →HSV colour space
3) Get the Hue 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.

B. Algorithm for Feature Authentication for authenticity checking

1) Pixel Selection Algorithm (Spatial Domain Embedding): The pixel selection algorithm for spatial domain embedding constitutes of some algorithm, these are-

For an Image of size m x n

I= Read the image

2) Algorithm for Cropping

a) for i=2:m-1

b) for j=2:n-1

c) crpI(i-1,j-1)=I(i,j);

d) end j

e) end i

crpI = Cropped Image

3) Algorithm for block processing

Size of cropped image crpI is m_1 X n_1 where m_1=m-2 and n_1=n-2

a) Initialize fi=0,fj=0

b) for i=1: floor (m_1/(4+1))

c) for j=1: floor (n_1/(4+1))

d) end j

e) fi=fi+(4+1);

f) fj=0;

g) end i

4) Algorithm for Embedding: At first convert the message image into a bit stream for embedding.

α_{ij}:=Add the squared value of integers up to the sum value which is below next of Pix_{ij} value

a) β_{ij}:=Add the squared value of integers up to the sum value which is next above of Pix_{ij} value

b) γ_{ij}:=(α_{ij}+ β_{ij})/2;

c) if Pix_{ij}<= γ_{ij}then δ_{ij}:=(Pix_{ij}–α_{ij}) else δ_{ij}:=(β_{ij}- Pix_{ij})

d) Calculate the value for bit stream of length n= 4,3,2 and 1

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

e) if $\sum^{4}$<= δ_{ij}then μ_{ij}:= $\sum^{4}$

elseif $\sum^{3}$<= δ_{ij} then μ_{ij} := $\sum^{3}$

elseif $\sum^{2}$<= δ_{ij} then μ_{ij} := $\sum^{2}$

elseif $\sum^{1}$<= δ_{ij} then μ_{ij}:= $\sum^{1}$

f) if Pix_{ij}<=γ_{ij}thenS_{ij}:=α_{ij}+μ_{ij} else S_{ij}:=β_{ij}-μ_{ij}

g) end j

h) end i

i) Stego image S generates

C. Feature Extraction from Retinal Image

Every retinal image constitutes of different type of cells which has been used in the system for authentication and those information are embedded through the transform domain.

1) Algorithm for Feature Extraction from Retinal Image

For an M X N *Retinal* image th

a) th1= thin image of image *retina* by binary image

b) Initialize N=3

c) n=(N-1)/2

d) for x:=(n+1+10):(s(1)+n-10)

e) for y:=(n+1+10):(s(2)+n-10)

set e=1

f) for k:=x-n:x+n

set f=1

g) for l=y-n:y+n

mat(e,f)=th1(k,l)

f=f+1

end l

h) e:=e+1

i) end k

j) if(mat(2,2)==0)

k) rods (x,y):=sum value of occurrence of zeros to mat

l) cons (x,y)= sum value of occurrence of zeros to mat

m) end y

n) end x

o) find rods and cons cell values

D. Proposed Method Algorithm for Data Hiding in Transform Domain

1) Pixel Selection Algorithm for Transform Domain Embedding: The pixel selection algorithm for Transform domain embedding constitutes of some algorithm, these are for an Image of size m x n.

Step1: I= Read the image

Algorithm for Cropping

for i=2:m-1

for j=2:n-1

crpI(i-1,j-1)=I(i,j);

end j

end i

crpI = Cropped Image

2) Algorithm for Block Processing using DCT

Size of cropped image crpI is m1 X n1 where m_1=m-2 and n_1=n-2

a) Initialize fi=0,fj=0,fqi=0,fqj=0;

b) for i=1: floor (m_1/(4+1))

c) for j=1: floor (n_1/(4+1))

d) for ii=1:4

e) forjj=1:4

blk=crpI((ii+1)+fi,(jj+1)+fj);

f) end jj

g) end ii

h) Dblk=dct2conversion of blk;

i) for ii=1:4

j) for jj=1:4

DcrpI((ii+1)+fqi,(jj+1)+fqj)=Dblk(ii,jj);

k) end jj

l) end ii

m) fj=fj+(4+1);

n) fqj=fqj+(4+1);

o) end j

p) fi=fi+(4+1);

q) fj=0;

r) fqi=fqi+(4+1);

s) fqj=0

t) end i

Let DcrpI = DCT processed image and rDcrpl = ignoring the element of top left corner of each block of DcrpI.

3) Algorithm for integer value ,sign and remainder extraction from DcrpI: Size of DCT processed image is m2 x n2

a) for i=1:m2

b) for j=1:n2

c) if DcrpI(I,j)>=0

VDcrpI(i,j)=floor(rDcrpI(i,j));

Sign(i,j)=1;

rem(i,j)= rDcrpI(I,j)-floor(rDcrpI(i,j));

d) else

VDcrpI(i,j)=floor(-rDcrpl(i,j));

e) Sign(i,j)=-1;

f) rem(I,j)=(-r Dcrpl(i,j))-floor(-rDcrpl(i,j));

g) end if

h) end j

i) end i

Integer value matrix is VDcrpI Sign matrix is Sign remainder matrix is rem

5) Algorithm for Embedding: At first convert the message image into a bit stream for embedding.

For an m_2 X n_2 matrix VDcrpIfori=1:m_2

for j=1:n_2

For each cell $Cell_{ij}$ in the matrix VDcrpI:-

a) α_{ij}:=Add the squared value of integers up to the sum value which is below next of $Cell_{ij}$ value(for example, $Cell_{ij}$=127 Then,$\alpha_{ij}=1^2+2^2+3^2+4^2+5^2+6^2=91< 127$)

b) β_{ij}:=Add the squared value of integers up to the sum value which is next above of $Cell_{ij}$ value (for example,$Cell_{ij}$=127 $\beta_{ij}=1^2+2^2+3^2+4^2+5^2+6^2+7^2=140 >127$)

c) γ_{ij}:=(α_{ij}+ β_{ij})/2;

d) if $Cell_{ij}<= \gamma_{ij}$thenδ_{ij}:=($Cell_{ij} - \alpha_{ij}$) else δ_{ij}:=(β_{ij}- $Cell_{ij}$)

e) Calculate the value for bit stream of length n= 4,3,2 and 1

$\sum^n:=x^n.(k+bit1)+\lambda x^{n-1}.(k+bit2)+x^{n-2}.(k+bit3)+\ldots\ldots\ldots+x.(k+bitn)$

f) if $\sum^4<= \delta_{ij}$then $\mu_{ij}:= \sum^4$

a. elseif $\sum^3<= \delta_{ij}$ then $\mu_{ij} := \sum^3$

b. elseif $\sum^2<= \delta_{ij}$ then $\mu_{ij} := \sum^2$

c. elseif $\sum^1<= \delta_{ij}$ then $\mu_{ij}:= \sum^1$

g) if $Cell_{ij}<= \gamma_{ij}$then$S_{ij}:= \alpha_{ij}+ \mu_{ij}$ else $S_{ij}:= \beta_{ij} - \mu_{ij}$

h) end j

i) end i

6) Algorithm for Stego Image Creation in Transform Domain

Algorithm for Sign Restoration

a) for i=1:m_2

b) for j=1:n_2

c) V(i,j)=sign(i,j) * (S(i,j)+rem(i,j))

d) end j

e) end i

7) Algorithm for Top Most Left Corner Value Restoration

a) for i=1:m_2

b) for j=1:n_2

c) V1(i,j)=mask11(i,j)+V(i,j);

d) end j

e) end i

mask11 *hold the only value of top most left corner of each block*

8) *Algorithm for Block Processing using Inverse DCT*

a) Initialize fi=0,fj=0,fqi=0,fqj=0;

i) for i=1: floor (m_1/(4+1))

ii) for j=1: floor (n_1/(4+1))

iii) for ii=1:4

iv) for jj=1:4

blk=V1((ii+1)+fi,(jj+1)+fj);

v) end jj

vi) end ii

vii) iDblk= inverse dct2conversion of blk

viii) for ii=1:4

ix) for jj=1:4

iDcrpI((ii+1)+fqi,(jj+1)+fqj)=iDblk(ii,jj)

x) end jj

xi) end ii

xii) fj=fj+(4+1)

xiii) fqj=fqj+(4+1)

xiv) end j

xv) fi=fi+(4+1)

xvi) fj=0;

xvii) fqi=fqi+(4+1);

xviii) fqj=0

xix) end i

9) *Algorithm for Ignored Cell Value Assignment*

a) Initialize fi=0,fj=0

b) for i=1: floor (m_1/(4+1))

c) for j=1: floor (n_1/(4+1))

d) for ii=1:4

e) for jj=1:4

I((ii+1)+fi,(jj+1)+fj)=iDcrpI(I,j);

f) end jj

g) end ii

h) fj=fj+(4+1)

i) end j

j) fi=fi+(4+1)

k) fj=0;

l) end i

m) Stego=I

n) Stego image is Stego.

10) *Algorithm for Extraction*

For an M X N Stego Image

fori=1:M

for j=1:N

For each cell $Cell_{ij}$ in Original image:-

a) α_{ij}:=Add the squared value of integers up to the sum value which is below next of $Cell_{ij}$ value

b) β_{ij}:=Add the squared value of integers up to the sum value which is next above $Cell_{ij}$ value

c) γ_{ij}:=(α_{ij}+ β_{ij})/2

d) if S_{ij}<= γ_{ij}thenδ_{ij}:=(S_{ij} - α_{ij}) else δ_{ij}:=(β_{ij}- S_{ij})

e) Get the equivalent bit stream of δ_{ij} and go for next pixel.
f) σ_{ij}=bit stream
g) msg:= Secret Message
h) ln:=length of msg
i) for k=1:ln
msg1:=ASCII of msg(k)
sh1=Convert msg1 to 8 bit value and shift 8-k bit to right
a(f)=sh1* (8 bit value of decimal value 1)
f:=f+1

VI. ANALYSIS OF THE RESULT

In this section the experimental results of the proposed method has been described. Table IV below shows the extracted features of different thumb image used for authentication as well as extracted secret message.

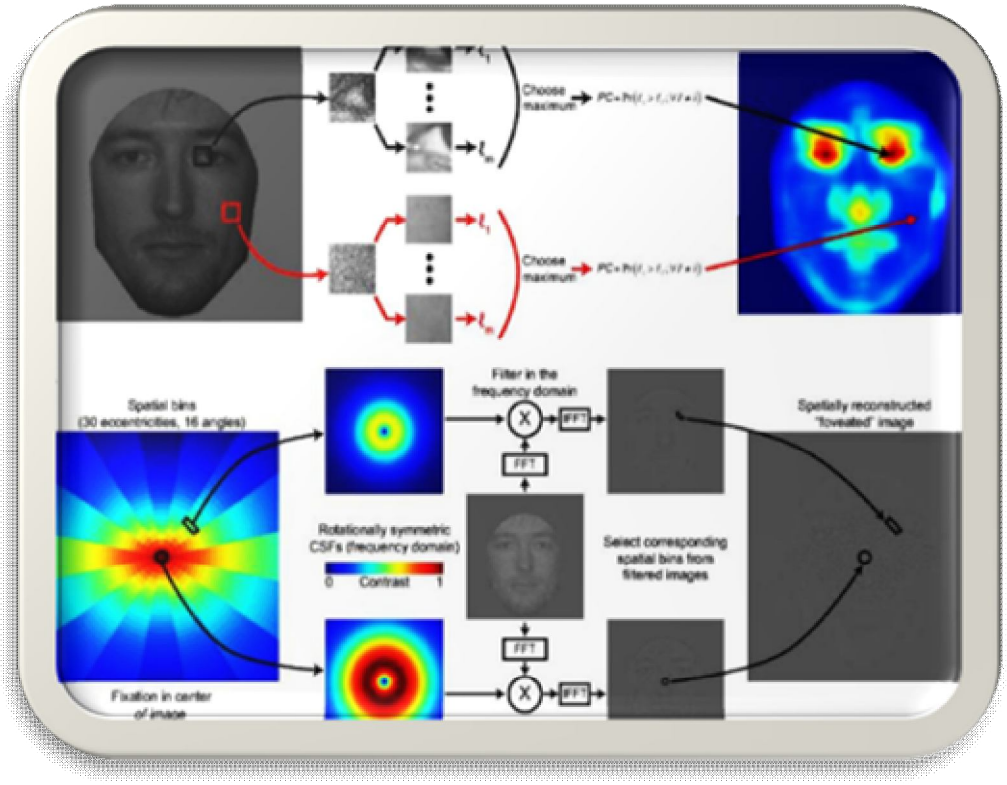
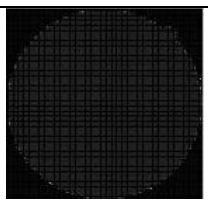
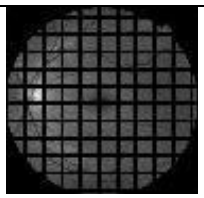
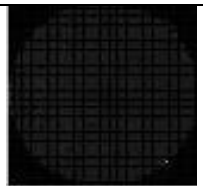
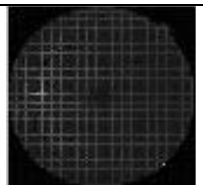


Fig 13. GUI of Feature Extraction from retina Image

TABLE IV
EXPERIMENTAL ELEMENTS

Authentication Image	Message Retinal Image	Resulting Extracted Feature Message of Retinal Image from Spatial Domain	Resulting Extracted Secret Message of Retinal Image from Frequency Domain
Retina1.jpg		RodCount= 5 ConeCount= 50	Message=AAAAAAAAAAAAA

Retina2.jpg		Rod Count= 27 ConeCount= 50	Message=AAAAAAAAAAAAA
Retina3.jpg		RodCount= 62 ConeCount= 180	Message=AAAAAAAAAAAAA
Retina4.jpg		Rod Count= 31 ConeCount= 259	Message=AAAAAAAAAAAAA

The experimental results of proposed method have been evaluated based on two benchmarks criteria. First one is the capacity of hidden data and the second one is the imperceptibility or the quality of the stego image. This method works in a combined approach of information hiding as well as authenticity checking. The capacity of hidden data depends upon the bit stream to be embed and embedding space which depends upon the pixel value so that capacity varies from message to message.
Imperceptibility or the quality of stego image produced by this method has been tested thoroughly based on various image similarity metrics namely MSE, PSNR, CORELATION, RMSE, SSIM, KLDIV and ENTROPY. Fig. 14 to 20 shows the graphical representation of calculated value of various similarity metrics for images.

A. Mean Square Error (MSE)

It is computed by averaging the squared intensity of the cover and stego image pixels. The "(10)" shows the MSE [39].

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

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

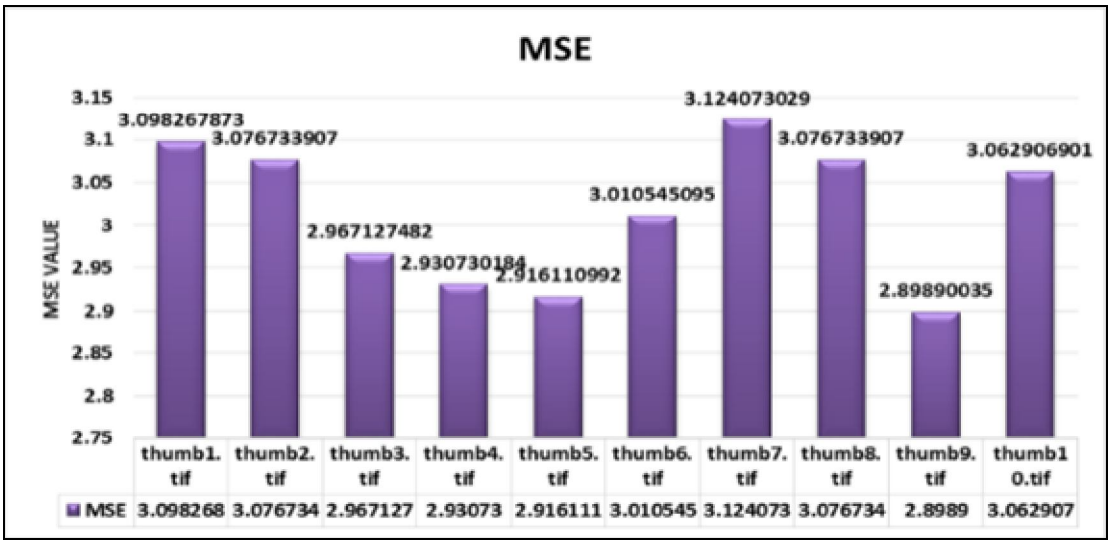


Fig 14: MSE for various Secret Images

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. PSNR [39] shows in equation"(11)".

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

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

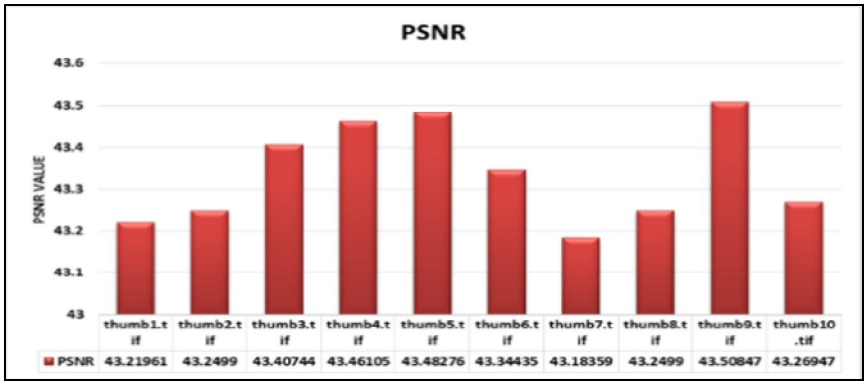


Fig 15: PSNR for various Secret Images

between cover and stego image, so HVS not identified the changes.

C. Correlations

Pearson's correlation coefficient [40] 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 equation"(12)".

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

The X_i and Y_i are the cover image and bar of X and Y are stego image positions. The correlation values are tens to 1 that means

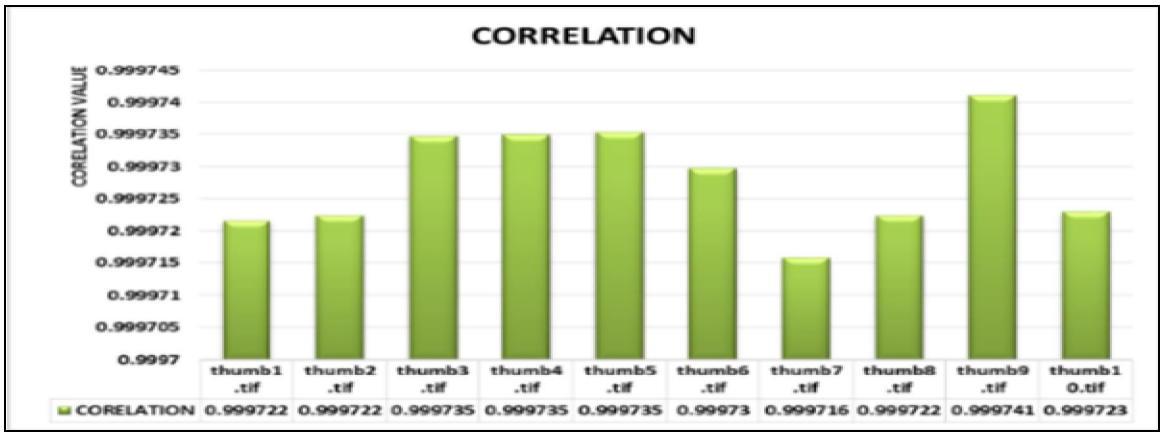


Fig 16: Correlation for various Secret Images

both the images are likely to same. RMSE [41] is one kind of measurement of difference between values of Cover Image and the values of Stego Image. The RMSE shows in equation"(13)".

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

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

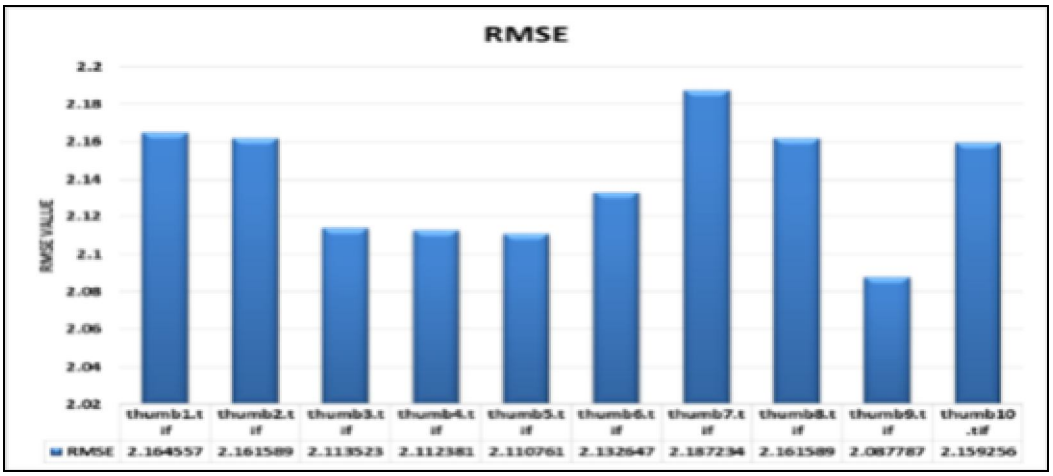


Fig 17: RMSE for various Secret Images

D. Structural Similarity Index (SSIM)

Wang et al. [42], proposed Structural Similarity Index concept between original and distorted image. The Stego and Cover images are converted into vectors. Then two means and two standard derivations and one covariance value are computed. Then the SSIM [42] computed between Cover and Stego images. SSIM shows in equation"(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.

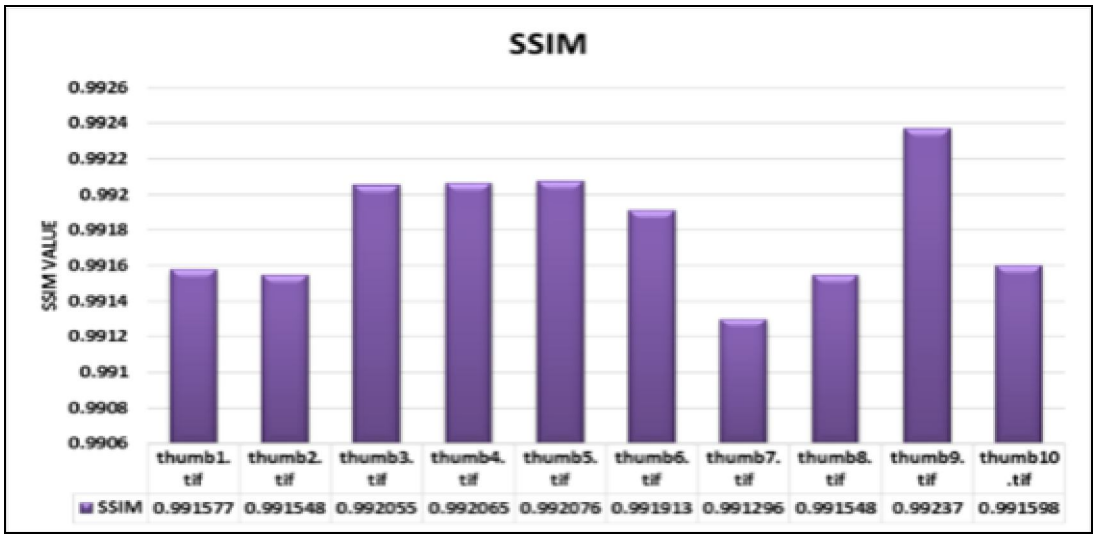


Fig 18: SSIM for various Secret Images

E.K L Divergence (KLDIVG)

With the help of probability density function (PDF) for each Image (cover and stego) we estimate the Kullback-Leibler Divergence [43]. KL divergence shows in equation"(15)".

$$D(p \parallel q) = \sum_x p(x) \log \frac{p(x)}{q(x)} \text{.....(15)}$$

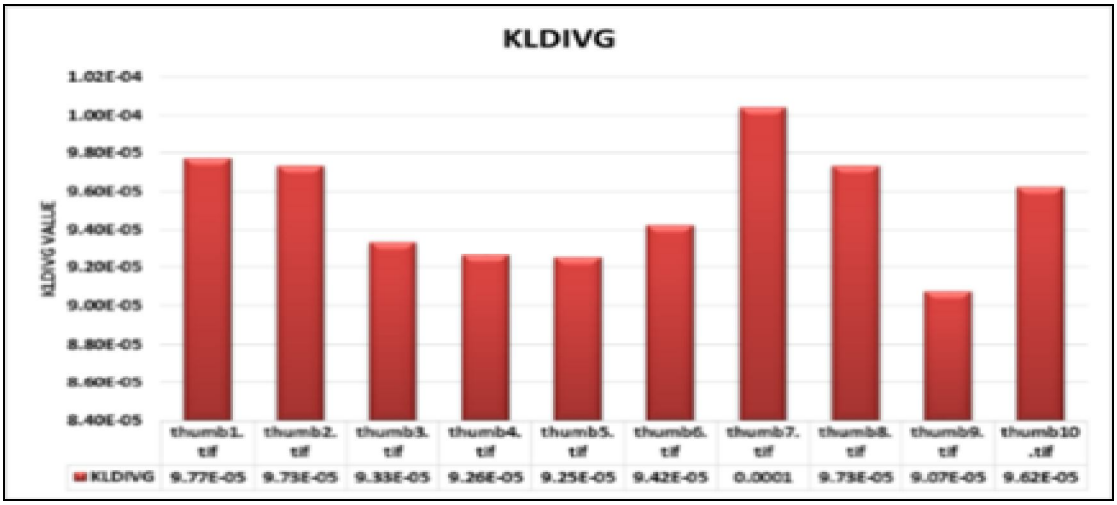


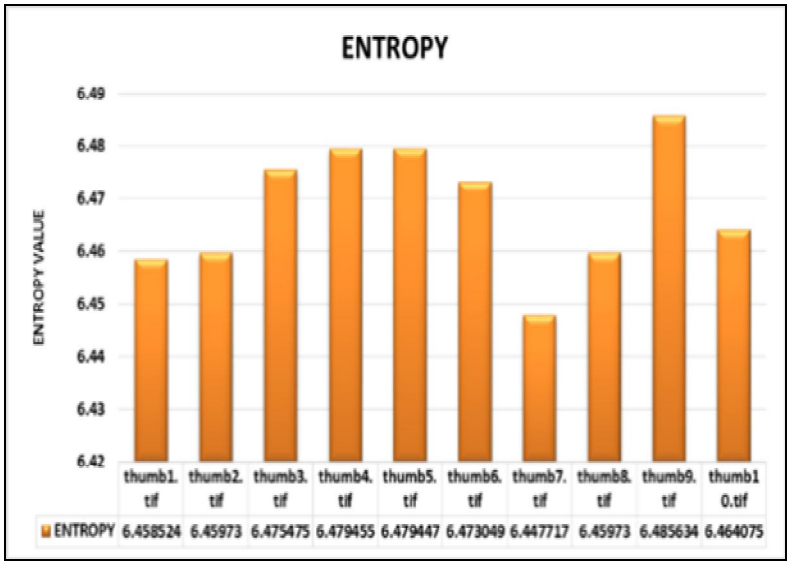
Fig 19: *K L Divergence for various Secret Images*

F. Entropy

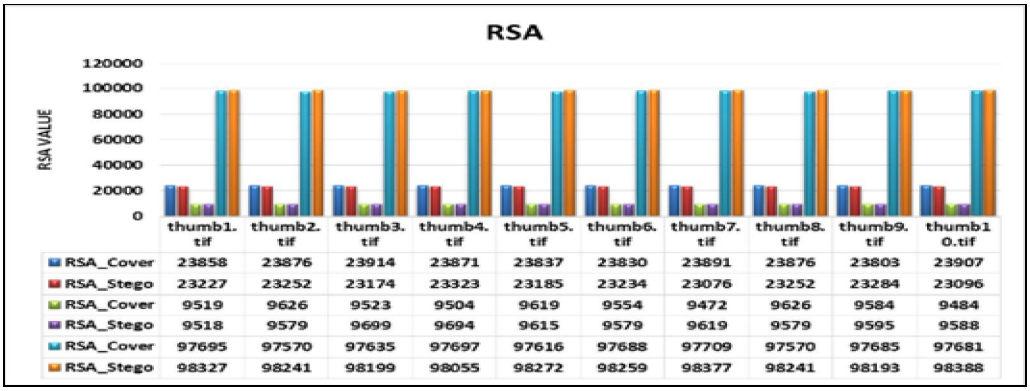
Entropy is a measure of the uncertainty associated with a random variable [44]. Here, a 'message' means a specific realization of the random variable. The equation"(16)" shows it.

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

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 [45]. Then Sample Pairs (SP) analysis was analyzed and reformulated by Dumitrescu et al. [46] 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. 21 shows the Analysis of attack of an RGB image as cover and stego image.



	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 21: RS Analysis for various Secret Images

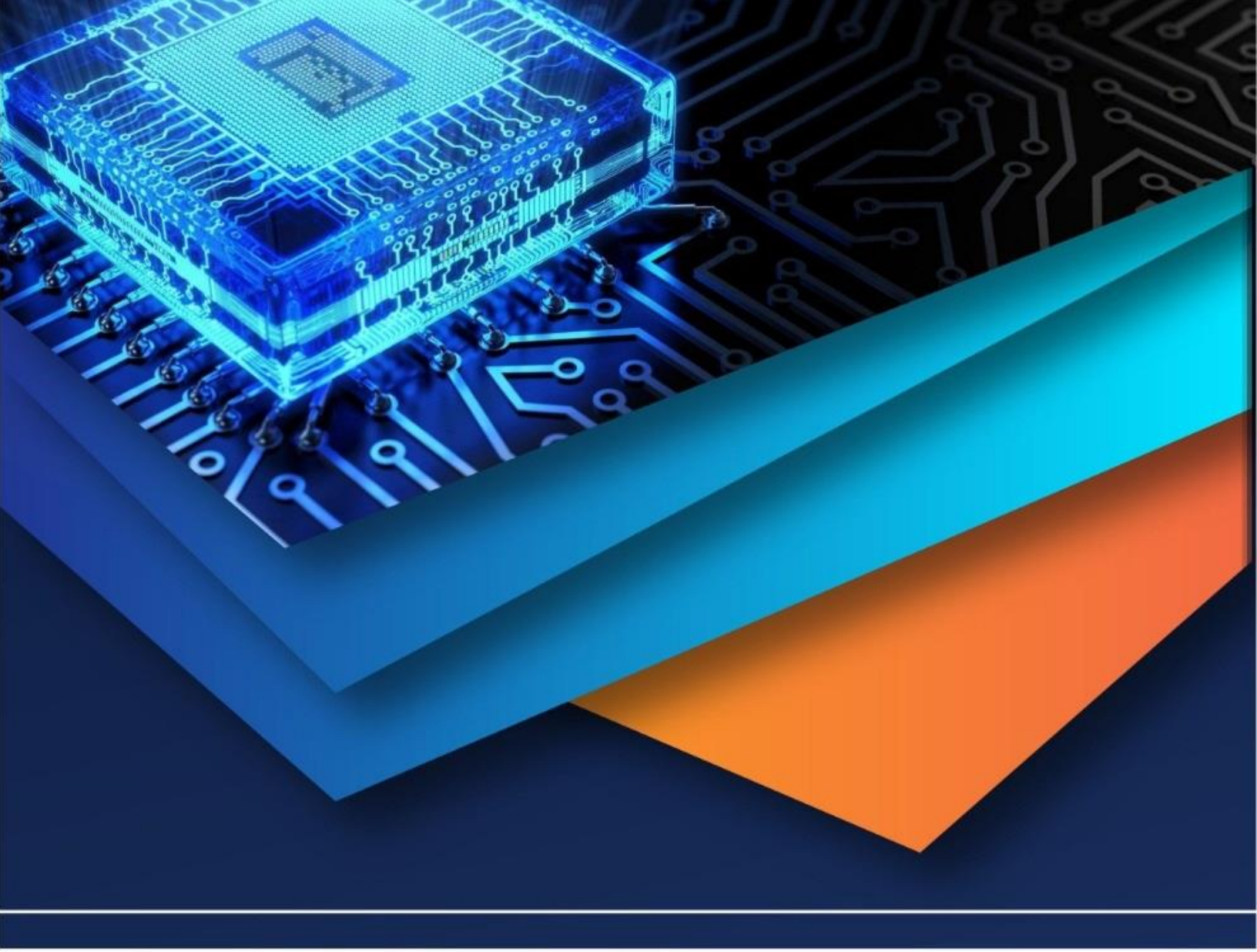
VII. CONCLUSION

In this paper a new and efficient approach of retinal biometric steganography technique has been proposed which works as a combination of spatial domain and transforms domain image steganography. This technique has been designed to incorporate both hiding and authentication aspects. Hiding of secret message has been done in frequency domain whereas authentication principle with the help of retina has been incorporated in spatial domain. In almost all the existing methods hiding of information has been done only either in spatial domain or in transform domain. In this work a humble attempt has been made to integrate the concept of information hiding and authentication principle with the aid of biometric security.

REFERENCES

[1] RJ Anderson, Stretching the Limits of Steganography, Information Hiding, Springer Lecture Notes in Computer Science,1174(1996) 39-48.
[2] JHP Eloff. T Mrkel. and MS Olivier. An overview of image steganography. In Proceedings of the fifth annual Information Security South Africa Conference., 2005.
[3] Jain.A.K, Hong.L, Pankanti.S: Biometric identification. Communications of the ACM 43 (2000) P. 91-98.
[4] 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.
[5] K. A. Rhodes, Information Security: Challenges in Using Biometrics, United States General Accounting Office, 2003.
[6] 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.
[7] 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.
[8] Souvik Bhattacharyya, Indradip Banerjee, AnumoyChakraborty, GautamSanyal. “Biometric Steganography Using Variable Length Embedding” Journal on WASETl Journal of Computer, Information, Systems and Control Engineering” Vol:8 No:4, 2014
[9] Y.K.Lee., L.H.Chen."High capacity image steganographic model". IEEE Proc.-Vision, Image and Signal Processing, 147:288–294, 2000.
[10] D.C. Wu.,W.H. Tsai. “A steganographic method for images by pixel value differencing”. Pattern Recognition Letters, 24:1613–1626, 2003.
[11] 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.
[12] 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.
[13] Souvik Bhattacharyya and GautamSanyal. Hiding data in images using pixel mapping method (pmm). In Proceedings of 9th annual Conference on Security and Management (SAM) under The World Congress in Computer Science, Computer Engineering, and Applied Computing (WorldComp 2010), Las Vegas, USA, July 12-15,2010.
[14] Souvik Bhattacharyya, Lalan Kumar and GautamSanyal, "A novel approach of data hiding using pixel mapping method (PMM)"International Journal of Computer Science and Information Security (IJCSIS), 8, 2010.

[15] Indradip Banerjee, Souvik Bhattacharyya and GautamSanyal, "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, Aug2013.
[16] Derek Upham. Jsteg, 2008.
[17] Allan Latham. Jphide., 2008.
[18] Andrew Westfeld. F5-a steganographic algorithm: high capacity despite better steganalysis. In Proceedings of the 4th Information Hiding Workshop, LNCS, volume 2137, pages 289–302, 2001.
[19] N. Provos. Defending against statistical steganalysis. In Proceedings of the 10th USENIX Security Symposium, pages 323–325, 2001.
[20] A. Sarkar K. Solanki and B. S. Manjunath. Yass: Yet another steganographic scheme that resists blind steganalysis. In Proceedings of the 9th Information Hiding Workshop, volume 4567 of LNCS, pages 16–31. Sprinnger, 2007.
[21] HJ Kim V Sachnev and R Zhang. Less detectable jpeg steganography method based on heuristic optimization and bch syndrome coding. In proceedings of ACM Workshop on Multimedia and Security, volume 4437 of Lecture Notes in Computer Science, pages 131–139, 2009.
[22] C. Wang and J. Ni. An efficient jpeg steganographic scheme based on the block-entropy of dctcoefficents. In proceedings of IEEE ICASSP, Kyoto, Japan, 2012.
[23] Souvik Bhattacharyya, A. Khan, GautamSanyal. "DCT Difference Modulation (DCTDM) Image Steganography". International Journal of Information & Network Security (IJINS), Vol 3, No 1 (2014).
[24] Ali Al Ataby and Fawzi Al Naima. A modified high capacity image steganography technique based on wavelet transform. The Int. Arab Journal of Information Technology,7:358–364, 2010.
[25] V. Kumar and D. Kumar. Performance evaluation of dwt based image steganography. In Proceedings of Advance Computing Conference (IACC), IEEE 2nd International, pages 223–228, 2010.
[26] 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.
[27] SubhraMazumdar; VenkataDhulipala. "Biometric Security Using Finger Print Recognition". University of California, San Diego. p. 3. Retrieved 30 August 2010.
[28] Retina and Iris Scans. Encyclopedia of Espionage, Intelligence, and Security. Copyright © 2004 by The Gale Group, Inc.
[29] R. Brunelli, Template Matching Techniques in Computer Vision: Theory and Practice, Wiley, ISBN 978-0-470-51706-2, 2009.
[30] MiroslavBača; Petra Grd and TomislavFotak (2012). "4: Basic Principles and Trends in Hand Geometry and Hand Shape Biometrics". New Trends and Developments in Biometrics. In Tech. Retrieved 1st December 2013.
[31] Shangling Song; Kazuhiko Ohnuma; Zhi Liu; Liangmo Mei; Akira Kawada; TomoyukiMonma "Novel biometrics based on nose pore recognition" 2009.
[32] Surya Prakash, UmaraniJayaraman&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.
[33] 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.
[34] 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.
[35] HomayoonBeigi, Speaker Recognition, Biometrics / Book 1, Jucheng Yang (ed.), Intech Open Access Publisher, 2011, pp. 3-28, ISBN 978-953-307-618-8.
[36] 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.
[37] Kumar, A., K. and K., V. Prathyusha, Personal authentication using hand vein triangulation, IEEE Trans. Image Process., Vol. 38, pp. 2127-2136, 2009.
[38] Indradip Banerjee, DipankarChatterjee, Souvik Bhattacharyya and GautamSanyal. Establishing User Authentication using Face Geometry, Journal on International Journal of Computer Applications (0975 – 8887) (IJCA). Vol. 92, No.16, April 2014.
[39] 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
[40] Guillermito(2004)."Steganography: a few tools to discover hidden data". Retrieved September, 2007, from http://www.guillermito2.net/stegano/tools/index.html
[41] J.L.Rodgers, J.L. and W.A.Nicewander, "Thirteen Ways to Look at the Correlation Coefficient", American Statistician 42, 59-66 (1995).
[42] Lehmann, E. L.; Casella, George (1998). "Theory of Point Estimation (2nd ed.)". New York: Springer. ISBN 0-387-98502-6.
[43] Pedro J. Moreno, Purdy Ho, NunoVasconcelos "A Kullback-Leibler Divergence Based Kernel for SVM Classification in Multimedia Applications" Conference: Neural Information Processing Systems - NIPS , 2003
[44] Claude E. Shannon, "A mathematical theory of communication", The Bell System Technical Journal., 27:379–423.
[45] Patricia R. Pereira. Andr R.S. Maral. "A steganographic method for digital images robust to rssteganalysis". Springer Lecture Notes in Computer Science, Vol. 3656., pages 1192–1199, 2005.
[46] 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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY