Multilayer Shelter Approach of Adaptive K-Bit Embedding for Biometric Template Protection

G.MaryAmirtha Sagayee[1], Dr.S.Arumugam[2], Dr.G.S.AnandhaMala[3]
[1]Associate Professor, Parisutham Institute of Technology & Science, Thanjavur
[2]Principal, Nandha Engineering College, Erode, India.
[3]Professor, St.Joseph's College of Engineering, Chennai, India.

ABSTRACT:

Biometric template protection has become an interesting research area to enhance the security of network communications, copyright protection etc. Steganography is an art of data concealing in such a way that forecloses the concealed messages. The simplest methodology to hiding the data within an image is called LSB substitution method. In this paper a novel noise guided clandestine data engrafting in a binding image is proposed. In the proposed method two copies of binding image is carried. A pixel value of one binding image is changed by the addition of Salt and Pepper noise and represented as noisy image. By reference of this noisy image the data needs to be secured is engrafted into the binding image. Besides protection of data, the quantity of data that can be concealed in a single bearing medium is also very important. This high engrafting capacity is attained by k- bits of clandestine messages are substituted in k- least significant bits of image pixels. The proposed scheme is examined and results compared with existing single bit substitution for the CASIA dataset biometric images. The experiment results affirm that the proposed scheme attains eminent data concealing capacity and maintains imperceptibility and dilutes the aberration among binding image and obtained stego image.

1. INTRODUCTION

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

Multimedia which needs to be secured may conceivably be encoded using cryptography or data hiding techniques including Steganography and digital watermarking. Cryptography encodes the confidential data into another form, either meaningful or not. A warden observing the communication channel is able to identify if a suspicious file is being transmitted. Steganography and digital watermarking used as means of data hiding techniques are popularly utilized for secure communication as mentioned in [1]. Types of cryptography techniques are categorized by the use of keys as well as pieces of information for extracting the protected file. Digital watermarking protects the multimedia by hiding authentication data either perceptually or inconspicuously while Steganography embeds the secret into another selection of multimedia avoiding visual attacks. All three methods are used for privacy and copyright protection, such as authentication of identifying data and intellectual property protection. The work presented here revolves around steganography in digital images.

Steganography, as already mentioned, consists of undetectably altering cover images to embed a message or image with the purpose of achieving secret communication. The properities of steganography are Embedding Effectiveness, Fidelity, Embedding Capacity and Embedding Efficiency.

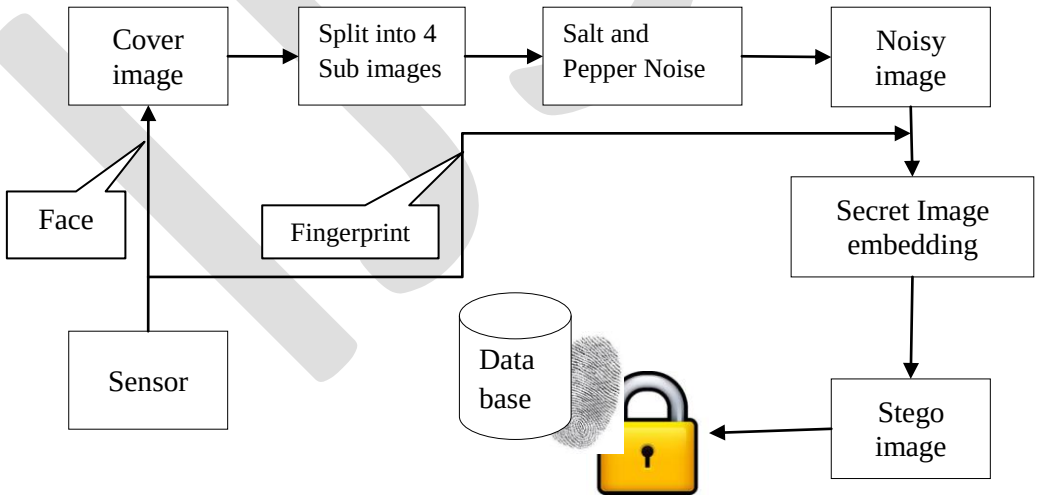

Fig.1. Proposed Architecture for steganography

When the people join into the cyberspace revolution, steganography become more important. It is the art of concealing information in ways that prevent the detection of hidden

messages. Some of the techniques used in Steganography are domain tools or simple system such as least significant bit (LSB) insertion. The Least Significant Bit (LSB) method [2] – [4] directly replaces the LSBs of the cover-image with the message bits. The advantage of LSB methods typically achieves high capacity. In this work, a Noise based embedding technique by using Salt and Pepper noise is proposed for steganography which is entirely different from the available techniques and the overall architecture is given in Fig.1.

2. SYSTEM DESIGN

In the Recent days, lots of steganography methods have been suggested. They are separated into two classification accomplished on their binding image domains: videlicet, spatial and frequency. In [5]-[7], the secret entropy are concealed in the pixels of the binding image by applying Least Significant Bit (LSB), Pixel Value Differencing (PVD), mod, run-length reversible and lossless information concealing based strategies. These strategies have been employed by many researchers to achieve beneficial imperceptibility with a more eminent consignment. In the frequency domain methods, the clandestine information's are concealed in the transformed coefficients of the binding image, where Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) play the domain converters [8]. Of the spatial domain stego methods, the LSB engrafting strategy has been broadly used to conceal clandestine information because of its simplicity and hasten of effectuation, which extends a more eminent concealment capability.

To improve the concealing capacity, more number of clandestine data should be engrafted into all binding image pixels [9]. Regrettably this scheme abbreviates the lineament of the consequent stego image. Besides the lineament, quantity of information that can be engrafted into an individual binding medium is also very significant.

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

In an existing LSB substitution techniques [10]-[13] preprocessing is done by dividing the binding image into blocks, dividing the binding image into color planes, adopting pixel indicator based substitution, Z- scanning, random walk methodology etc,. In our paper, binding image of proposed system is preprocessed by the addition of Salt and Pepper Noise. Noise with defined density is added with the copy of binding image.

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

2.1. Enhancement of Proposed System

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

2.2. Noise guided stegging

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

2.3.Adaptive K- bit Embedding

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

It can be easily understand that the pixel value is changed in the noisy image based on the added Salt and Pepper noise. Now the secret data is embed into the cover image based on this changes. That is secret data is embed into the cover image by the varied pixel positions in the

reference image. In this proposed method, three different bits of secret data is embedding as per the values in the noisy image.

If the pixel value of noisy image and cover image are same then two bits of data is embed into the cover image. If a pixel is added with salt then that value becomes zero and 1 bit of data is embed. Three bits of data is embedding into the cover image for the pepper added pixel values. For our convenient a cover image of size 256*256 is taken, therefore the pixel value of salt added portion is 0 and the pixel value of Pepper added portion is 255.

3. ALGORITHM FOR PROPOSED METHOD

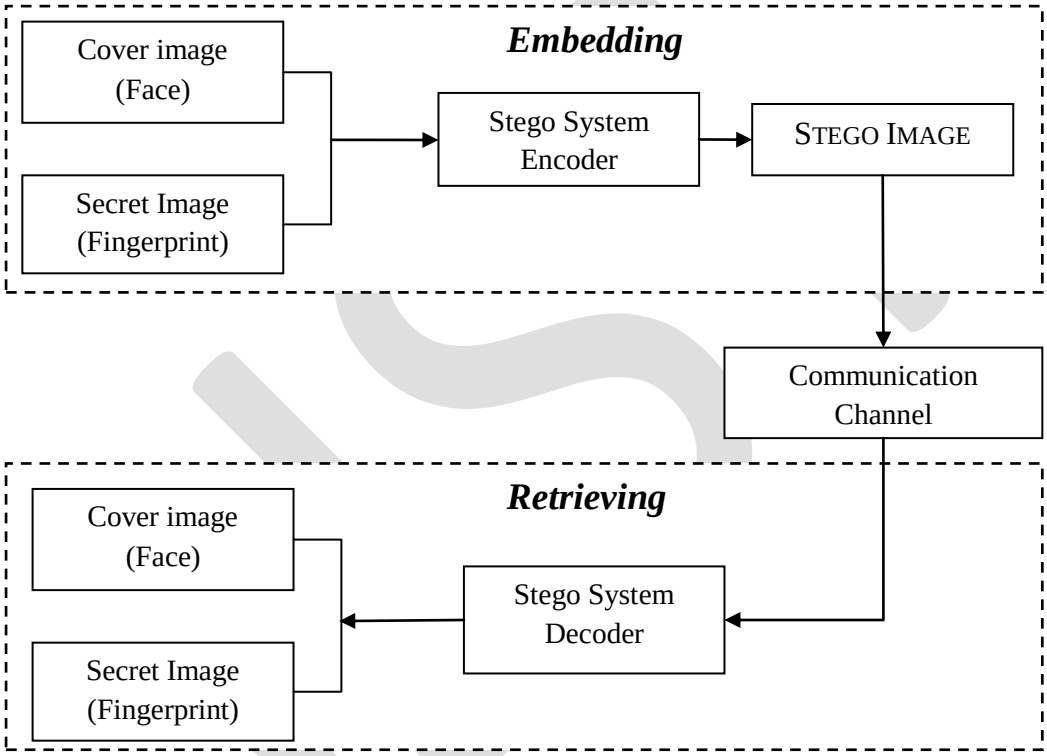

Fig 2. Proposed system for Embedding and retrieving

System design comprises two contributions such as embedding and retrieving as shown in Fig.2. In an embedding part, fused finger print (secret data) and Face (cover image) are afforded to the stego system encoder as inputs. Stego system encoder adopts our proposed system for the process of embedding the secret data into the cover image with the support of noisy image. In a retrieving part the reverse process of above is done for acquiring the transmitted clandestine data.

3.1.Functional Module for Engrafting

Procedure done in stego system encoder has explicated in this division. As cited earlier stego system encoder utilizes the proposed schemes, Noise guided stegging and Adaptive K- bit engrafting. In a preprocessing step Salt and Pepper Noise is added with the binding image. Then the three sets of pixels in the noisy image are used to lead the adaptive engrafting scheme for concealing the clandestine data into the binding image as shown in Fig.3 .

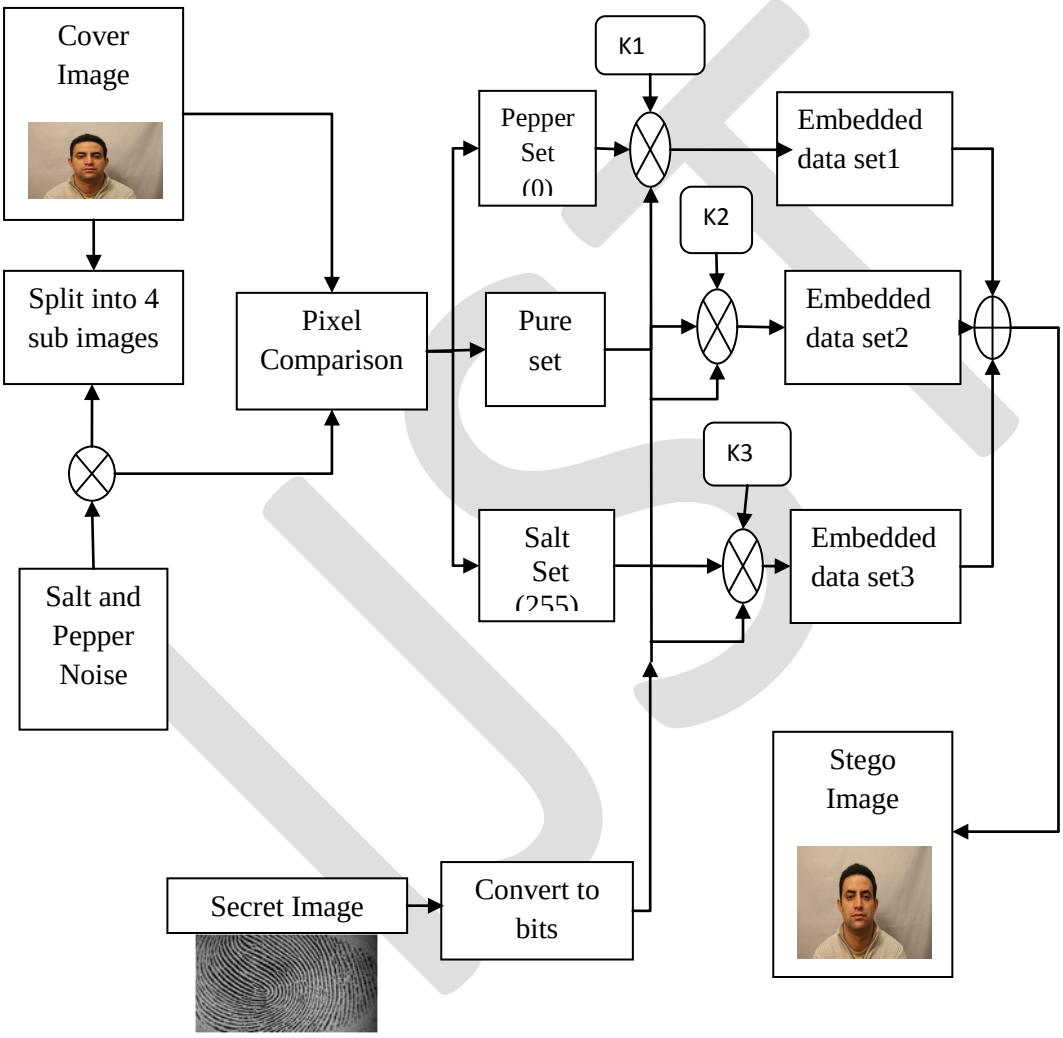

Fig 3.Stego System Encoder

Algorithm:

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

Step-2: Find the binary bit stream of secret image.

Step-3: Interpret the cover image (A) for concealment and subdivide it into 4 images.

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

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

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

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

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

Step-6: Done the engrafting through the decision making as follows

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

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

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

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

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

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

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

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

Step-11: Store the resultant image in database.

3.2.Functional Module for Retrieving

To retrieve the engrafted clandestine data, Obtained Stego and Binding images are given as an input to the stego system decoder. Stego image is divided into three sets as done in stego system encoder. Now, the exact adaptive key engrafted in stego system encoder must to be given to retrieve the exact clandestine data as mentioned in Fig.4.

Algorithm:

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

Step-2: Interpret the stego image from Database.

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

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

Step-5: Clandestine data retrieving

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

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

Ste9-8: Convert the retrieved bits into characters.

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

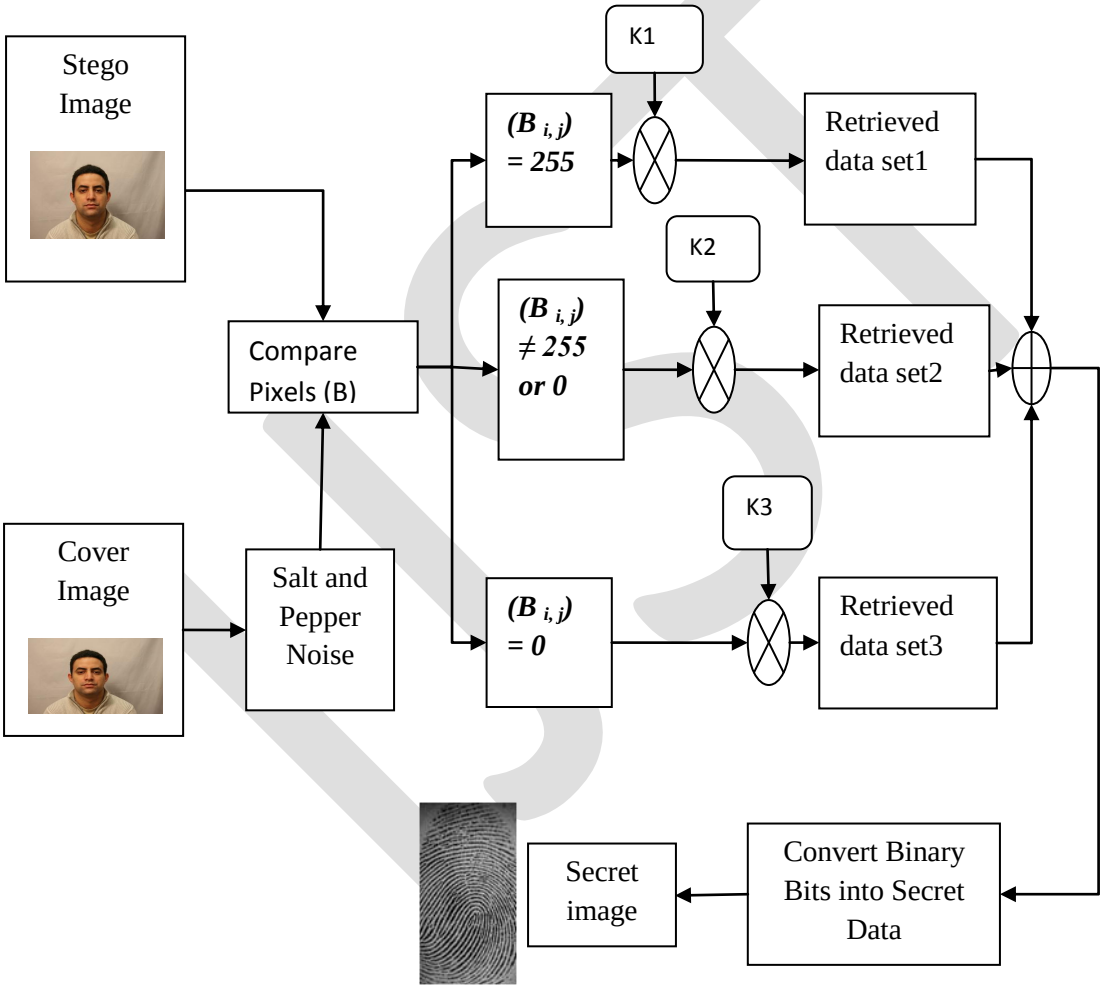

Fig 4.Stego System Decoder

4. Testing Measures

4.1.Bits Per Pixels (BPP)

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

$$BPP = (\frac{C}{P}) \quad \ldots (4.1)$$

Where,

C= total number of bits engrafted

P= M * N

M= Number of pixels in row of 2D image

N= Number of pixels in column of 2D image

4.2.Mean Square Error (MSE)

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

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(O_{i,j} - A_{i,j})^2 \quad \ldots (4.2)$$

Where,

M= Number of pixels in row of 2D image

N= Number of pixels in column of 2D image

4.3.Peak Signal to Noise Ratio (PSNR)

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

$$PSNR = 10log_{10}(\frac{I_{max}^2}{MSE}) \text{ dB} \quad \ldots (4.3)$$

I_{max} = Maximum intensity of 2D image.

5. RESULTS AND CONCLUSION

The experiments were simulated by using CASIA database. The cover image taken here is face and secret image is fingerprint of a same person. The obtained results are discussed below,

(a) (b)

Fig.5. a) Cover image b) secret image

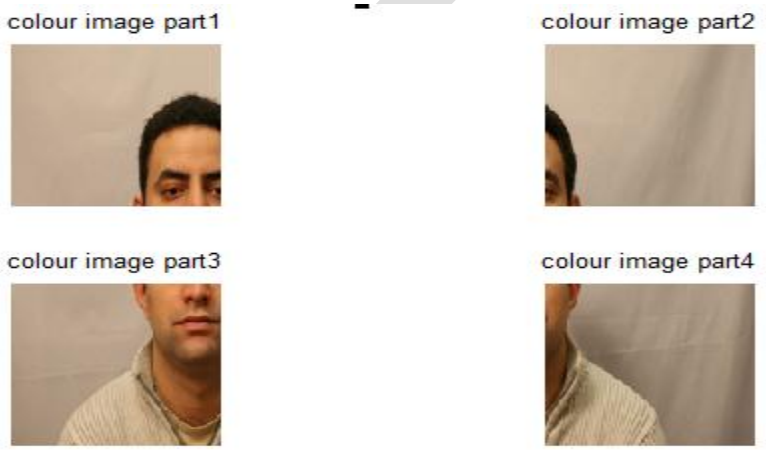

Fig 6. Sub images

Fig.7. Noisy image

Issue 4 volume 3, May-June 2014
ISSN 2249-9954

Fig.8. Stego image

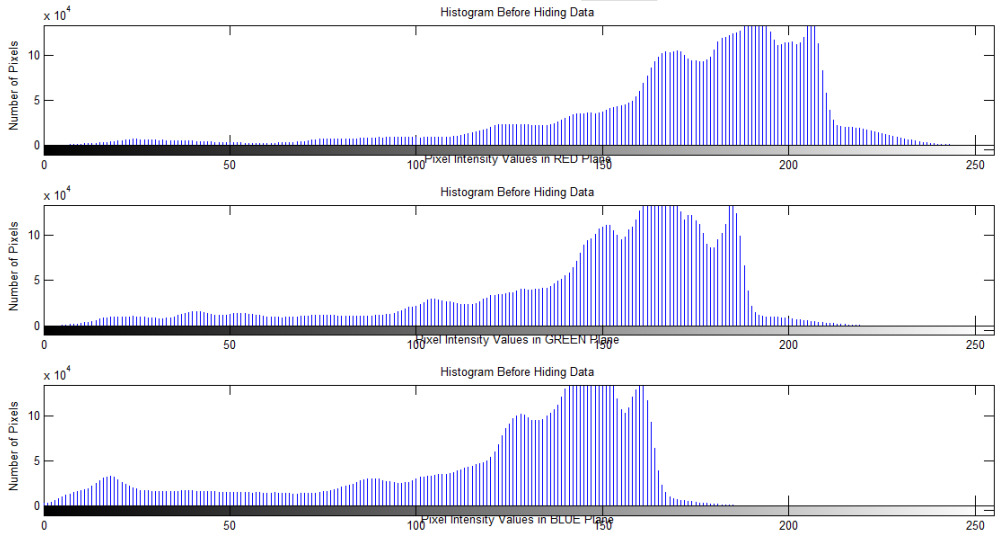

Fig.9. Histogram before hiding for R, G and B plane

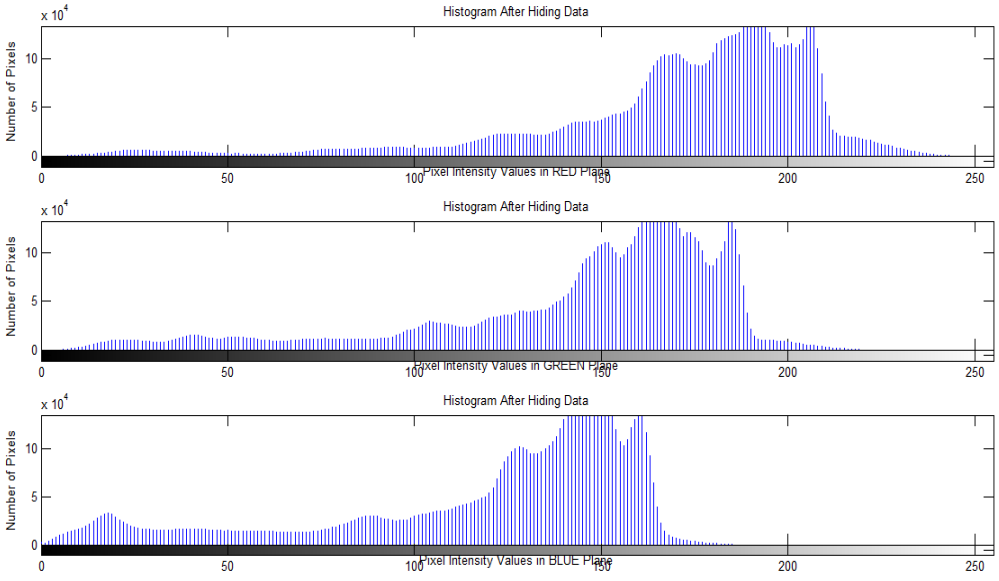

Fig.10. Histogram after hiding for R, G and B plane

From Fig.9 and 10, it can be recognized that there is no visual difference between the resultant image and the binding image. The proposed Noise Guided Random Stegging with adaptive K- bit engrafting Stego system has been enforced in four sub images. The Capacity of the stego images has been assessed and the consequences are evidenced in tables 1- 3. Initially, the stego image capacity was gauged by the simple LSB substitution with standardized key engrafting in all the pixels and the consequences are exhibited in table 1. To establish the enhanced concealing capacity and quality of stego image developed by the proposed approach, the estimated BPP, Total engrafting capacity, MSE and PSNR of the stego image are compared with the results presented in table 1.

TABLE.1: BPP, MSE, PSNR, CONCEALING CAPACITY OF EXISTING

Binding image	Measure	Number of Clandestine Data bits embedded			
		K=1	K=2	K=3	K=4
User 1	Total No. of Bits embedded	42821	85642	128463	171284
	BPP	0.2178	0.4356	0.6534	0.8712
	MSE	0.3657	0.1738	0.7282	2.7769
	PSNR	62.5657	55.7305	49.5128	43.6988
User 2	Total No. of Bits embedded	42882	85764	128646	171528
	BPP	0.2181	0.4362	0.6543	0.8724
	MSE	0.0363	0.1566	0.7917	3.5750
	PSNR	62.5741	56.1913	49.2042	42.7309

TABLE.2: PERFORMANCE MEASURES FOR USER 1

Adaptive K-bit K= k1-k2-k3	Total No. of bits Engrafted	BPP	MSE	PSNR
1-2-3	401230	2.0408	0.2736	52.7179
3-2-1	400793	2.0385	0.2632	53.7697
2-1-3	212480	1.0807	0.2470	54.2049
3-1-2	212319	1.0799	0.2444	54.2495

In table.1 it can be noticed that the concealing capacity and BPP are raised from k=1 to k=4, but values of MSE and PSNR diminished respectively. This fluctuation should not be the case for a amend stego system. A good system must have high concealing capacity as well as superiority stego image. This retreat in the existing simple LSB substitution with standardized key engrafting can be defeat by employing the proposed Adaptive K- bit Engrafting technique.

Table 2 and 3, demonstrates that the proposed scheme has the extremely high data concealing capacity. Adaptive algorithm assures that the quality of the resultant stego image is not compensated.

TABLE.3: PERFORMANCE MEASURES FOR USER 2

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

CONCLUSION

The proposed healthy stego system has multilayer shelter against different attacks. For each module, the proposed technique that leads in the maximum BPP, minimum MSE and good PSNR values is adopted here, there by augmenting the concealing capacity of the stego image.

Moreover, splicing the binding image with three dissimilar pixel sets by using noise guided image meliorates the protection of the vital message because only the authorized user has the key to the correct compounding of data set pixel emplacements and binary pattern applied in each combination. Furthermore the noise guided stegging technique extends significantly improved security without markedly conciliatory the payload. In addition, choice of engrafting adaptive key and the pixels sets are allowed for user defined decision making instead of manual and predefined decisions. So the attacker can't able to modify or misuse the biometric database.

REFERENCES

[1] Amitava Nag, Saswati Ghosh, "An Image Steganography Technique using X-Box Mapping", ISBN: 978-81-909042-2-3 2012 IEEE.

[2] M. Khodaei, K.Faez, "New adaptive steganographic method using least significant-bit substitution and pixel-value differencing", published in IET Image Processing, December 2012.

[3]Marghny Mohamed, Fadwa Al-Afari,"Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation", International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011.

[4] S. M. Masud Karim, Md. Saifur Rahman, "A New Approach for LSB Based Image Steganography Using Secret Key", 987-161284-908-9/11 2011 IEEE.

[5]Rengarajan Amirtharajan, Aishwarya G "Optimum Pixel and Bit location for Colour Image Stego- A Distortion Resistant Approach"

[6] Supriya Rai and Ruchi Dubey, "A Novel Keyless Algorithm for Steganography", 978-1-4673-0455- 9/12 2012 IEEE.

[7] Wien Hong*, "Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique",2012 Elsevier Inc.

[8]Unseen: An Overview of Steganography and Presentation of Associated Java Application C-Hide. http://www.cse.wustl.edu/~jain//cse57109/ftp/index.html#1

[9] J. AnitaChristaline1, D.Vaishali, "Image steganographic techniques with improved embedding capacity and robustness", 978-1-4577-0590-8/11 2011 IEEE.

[10]R.Amirtharajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, "Colour Guided Colour Image Steganography", Universal Journal of Computer Science and Engineering Technology, ISSN: 2219-2158.

[11] Gandharba Swain and Saroj Kumar Lenka, "A Novel approach to RGB channel Based Image Steganography Technique", International Arab Journal of e-Technology, vol. 2, No. 4, June 2011.

[12] Gandharba Swain and Saroj Kumar Lenka,"A Better RGB Channel Based Image Steganography Technique," CCIS 270, pp. 470–478, Springer-Verlag Berlin Heidelberg 2012.

[13] Joan Condell, Abbas Cheddad, Kevin Curran, Paul McKevitt, "Digital image steganography: Survey and analysis of current methods," 0165-1684, 2009 Elsevier B.V. International Journal of Computer Applications (0975 – 8887)Volume 10– No.7, November 2010.