A Novel Noise Guided Random Stegging with Adaptive K-bit Engrafting to Enhance Eminent Concealing Capacity

J.Jayaseelan[1]
M.E. Communication Systems,
Parisutham Institute of Technology & Science, Affiliated to Anna University Chennai.
Tamil Nadu- India
Email: jayaseelan.j89@gmail.com

B.Kruthika[2]
Assistant Professor,
Parisutham Institute of Technology and Science, Affiliated to Anna University Chennai.
Tamil Nadu- India
Email: kruthikabme@gmail.com

***Abstract*-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 noises such as Salt & Pepper, Gaussian, Etc., 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, where k alters from 1 to 3 depending on the added noise. The proposed scheme is examined and results compared with existing single bit substitution for the test images temple, Gandhi, baboon and Lena. 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**

Index terms: Binding image, clandestine data, k- bit embedding, Noise guided stegging, stego image

I. INTRODUCTION

The shelter of confidential data has long been a major pertain. To defend this extremely confidential data from being tapped, altered, or utilized by unauthorized persons, we required having methods for attaining data protection.

The most well known method for data protection is using Data Concealing, which is the procedure of concealing details of an article or function. A significant method of data concealing is *steganography* [1- 5]. It is the skill of concealing data. It conceals the clandestine message within the emcee data set and makes its presence imperceptible. The main objective of steganography is to avoid absorbing hunch to the existence of a concealed content. [6-9]

In steganography, the binding medium is the file in which we will hide the clandestine data. The resultant file is the stego medium. The binding mediums are typically image or audio files. [1, 2, 10-14]

II. RELATED WORKS

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 [1, 2, 15-19]. In the spatial domain, the secret entropy are concealed in the pixels of the binding image by applying Least Significant Bit (LSB) [20, 21], Pixel Value Differencing (PVD) [22], 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 [18, 19, and 27]. 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 [28]

To improve the concealing capacity, more number of clandestine data should be engrafted into all binding image pixels. 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 [23-24, 26].

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 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 & 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*.

III. PROPOSED METHODOLOGY

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

A. *Noise guided stegging*

Salt & Pepper noise is a random noise with ON & OFF Pixels. It modifies the pixel values into either Zero or Maximum intensity of the image. In this proposed scheme Salt & 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 & pepper Noise with determined density is contributed with the input binding image.

This noise added binding image is represented as *guiding image* or *reference image* with three dissimilar set of pixels they are Salty pixels, peppery pixels and pure pixels. Corresponding pixels assesses are Zero, Maximum (255 for 256 * 256 images) and similar as like binding image respectively. Instead of fixed decision making for the number of pixels to be engrafted into a binding image, our proposed scheme avails the user defined decision making potentiality. A sender or engrafting authority can decide the pixels should be utilized for engrafting. Sender has the following choices for concealing the clandestine data: select salty pixels of binding image, peppery pixels of binding image, pure pixels of binding image, both salt & pepper, both salt & pure pixels, Pepper & Pure pixels. So the pixels with engrafted clandestine data are extremely insufferable to accumulate because of the randomization of proposed methodology. Eventually this noise guided random stegging system meliorates the quality of the resultant stego image with high imperceptibility factor.

B. *Adaptive K- bit Engrafting*

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 from 1-3. Let us assume the sender has decided to engraft all three available set of pixels in a binding image with the following order: salty pixels, peppery pixels, pure pixels. Now the sender can engraft the clandestine data with the following bit sets as respective of above order:
1-2-3, 1-3-2, 2-1-3, 2-3-1, 3-1-2, and 3-2-1. This ability attains the eminent concealing capacity without conciliatory the quality of stego image. This decision making also made as user defined.

C. *System Design*

System design comprises two contributions such as engrafting and retrieving as shown in fig.1. In an engrafting part, encrypted secret data and binding image are afforded to the stego system encoder as inputs. Stego system encoder adopts our proposed system for the process of engrafting the secret data into the binding image with the support of guiding image. In a retrieving part the reverse process of above is done for acquiring the transmitted clandestine data.

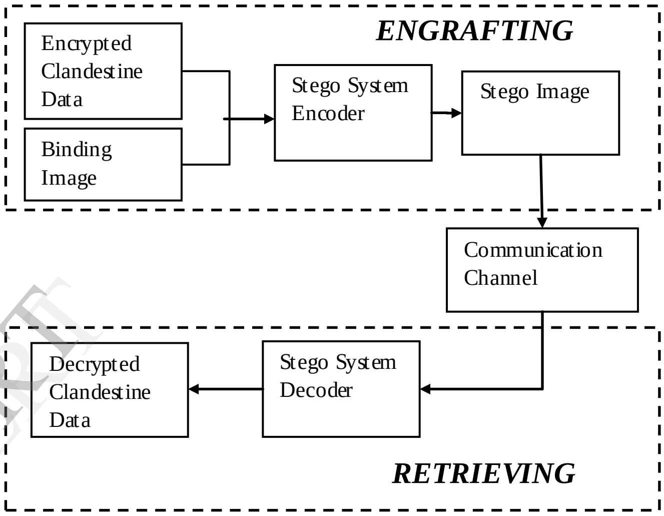

Fig.1: System Design

D. *Functional module*

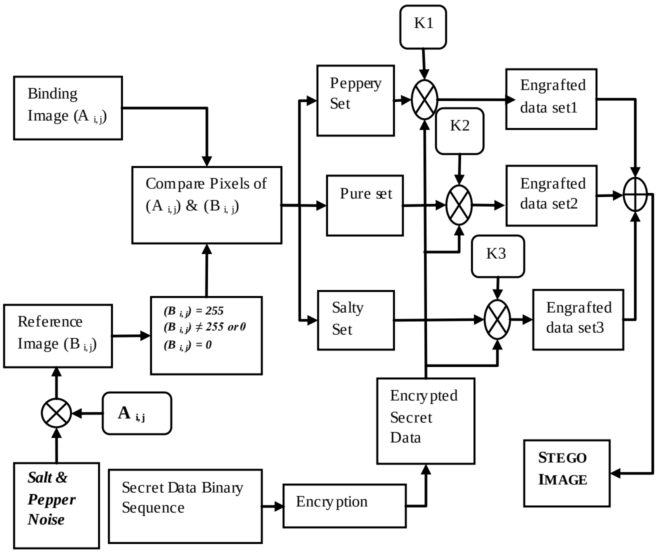

Fig.2: Stego System Encoder Functional Module

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 & 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. 2.

E. Algorithm for Engrafting

Inputs:

1. Binding image (A_{ij})
2. Clandestine data bit stream (F)
3. Adaptive key for K-bits
4. Encryption key

Outputs:

1. Stego image (O_{ij})

Algorithm:

Step-1: Encrypt the clandestine data (F) by offering a Symmetric key.

Step-2: Find the binary bit stream of clandestine data (F)

Step-3: Interpret the binding image (A_{ij}) for concealment

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 Guiding image (B_{ij})

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

If B_{ij} ==0 then Salty pixels ($B_{s,ij}$),
Else, if B_{ij} == 255, then Peppery pixels ($B_{p,ij}$)
Else, if Bij == Aij then Pure pixels ($B_{u,ij}$)

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

If the key for $B_{s,ij} \neq B_{u,ij} \neq B_{p,ij} \neq 0$, then choose the entire binding image and separate them into three sets based on the pixel values.

Else, if the key for $B_{s,ij} \neq B_{u,ij} \neq 0$ & $B_{p,ij} = 0$, then choose and separate the pixels of Salty & pure and leave the Peppery pixels in binding image.

Else, if the key for $B_{s,ij} \neq B_{p,ij} \neq 0$ & $B_{u,ij} = 0$, then choose and separate the pixels of Salty & Peppery and leave the Pure pixels in binding image.

Else, if the key for $B_{p,ij} \neq B_{u,ij} \neq 0$ & $B_{p,ij} = 0$, 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. Then the maximum key possibilities are as follows,

k1 = key for peppery pixels
k2 = key for pure pixels
k3 = key for salty pixels
K= k1, k2, k3; K alters from 1 to 3.

K= 1,2,3; 1,3,2; 2,1,3; 2,3,1; 3,1,2; 3,2,1

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 (O_{ij})

F. Algorithm for clandestine data retrieving

Inputs:

1. Stego image (O_{ij})
2. Guiding image (B_{ij})
3. Adaptive K-bit key
4. Decryption key

Output:

1. Retrieved clandestine data (F)

Algorithm:

Step-1: Interpret the stego image (O_{ij})

Step-2: Interpret the Guided image (B_{ij})

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

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

Step-5: Clandestine data retrieving:

If k1 is 3 then retrieve three MSBs of Clandestine data (F) from the LSBs of Stego image (O_{ij})
Else, if k1 is 2 then retrieve 2bits of F
Else, if k1 is 1 then retrieve 1bit of F
Else, if k1 is 0 then no data has engrafted into that corresponding pixel.

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: Decrypt the retrieved data by providing the same key as used in encryption.

IV. TESTING MEASURES

A. 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,

$$\text{BPP} = \left(\frac{C}{P}\right) \qquad \dots (1)$$

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

B. 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.

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

Where,

M= Number of pixels in row of 2D image
N= Number of pixels in column of 2D image

C. *Peak Signal to Noise Ratio (PSNR)*

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

$$\text{PSNR} = 10log_{10}\left(\frac{I_{max}^2}{MSE}\right)\text{ dB} \qquad \ldots (3)$$

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

V. RESULTS & DISCUSSION

The proposed Noise Guided Random Stegging with adaptive K- bit engrafting Stego system has been enforced in four unlike binding images. The Concealing Capacity of the stego images has been assessed and the consequences are evidenced in tables 2-5. Initially, the stego image concealing 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.

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. Here the clandestine data with the size of 71.5kb is engrafted into Temple and baboon binding images.

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

Binding image	Measure	Number of Clandestine Data bits engrafted			
		K=1	K=2	K=3	K=4
Temple	Total No. of Bits Engrafted	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
Baboon	Total No. of Bits Engrafted	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

Tables 2 to 5, 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.2: PERFORMANCE MEASURES FOR BINDING IMAGE TEMPLE

Binding image size: 35.6kb , Clandestine data size: 71.5kb				
Adaptive K-bit Clandestine data K= k1-k2-k3	Total No. of bits Engrafted	BPP	MSE	PSNR
1-2-3	401230	2.0408	0.8736	48.7179
3-2-1	400793	2.0385	0.8632	48.7697
2-1-3	212480	1.0807	0.2470	54.2049
3-1-2	212319	1.0799	0.2444	54.2495

TABLE.3: PERFORMANCE MEASURES FOR BINDING IMAGE BABOON

Binding image size: 192kb , Clandestine data size: 71.5kb				
Adaptive K-bit Clandestine data K= k1-k2-k3	Total No. of bits Engrafted	BPP	MSE	PSNR
1-2-3	401345	2.0413	0.8649	48.7612
3-2-1	401561	2.0425	0.8603	48.7850
2-1-3	213290	1.0848	0.2513	54.1287
3-1-2	213274	1.0848	0.2569	54.0379

TABLE.4: PERFORMANCE MEASURES FOR BINDING IMAGE LENA

Binding image size: 15.6kb , Clandestine data size: 71.5kb				
Adaptive K-bit Clandestine data K= k1-k2-k3	Total No. of bits Engrafted	BPP	MSE	PSNR
1-2-3	401478	2.0420	0.8793	48.6895
3-2-1	402009	2.0447	0.8697	48.7372
2-1-3	213136	1.0840	0.2489	54.1717
3-1-2	213599	1.0864	0.2555	54.0659

TABLE.5: PERFORMANCE MEASURES FOR BINDING IMAGE GANDHI

Binding image size: 5.96kb , Clandestine data size: 71.5kb				
Adaptive K-bit Clandestine data K= k1-k2-k3	Total No. of bits Engrafted	BPP	MSE	PSNR
1-2-3	402546	2.0475	0.8820	48.6763
3-2-1	405175	2.0608	0.9017	48.5879
2-1-3	215248	1.0948	0.2540	54.0854
3-1-2	216278	1.1000	0.2905	53.5943

The images of the representing binding images with guiding and stego images are shown in figures 3 to 6. It can be recognized that there is no visual difference between the resultant image and the binding image.

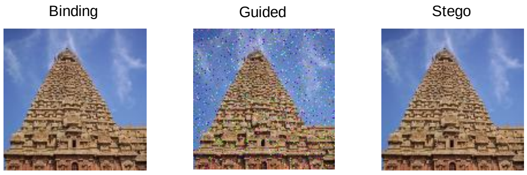

Fig.3: Results by applying Temple image

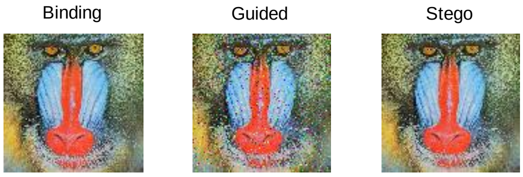

Fig.4: Results by applying Baboon image

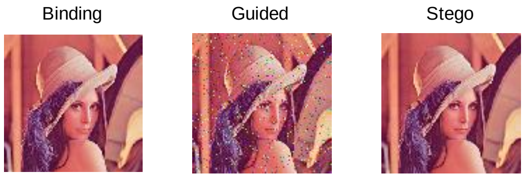

Fig.5: Results by applying Lena image

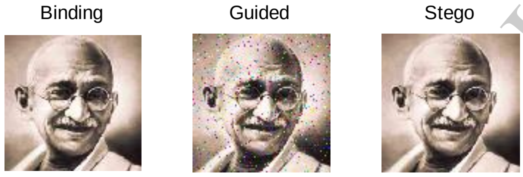

Fig.6: Results by applying Gandhi image

In all the above images Salt & Pepper noise is added with the density of 0.04. This density is user defined based on the requirement. If a sender demands more pixels with modified intensity then the density can be raised.

VI. Security Analysis

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. Ultimately, by imparting flexibility in the choice of terminus a quo of the engrafting pixel set, this method assures huge security and invulnerability.

The paces necessitated in the protection mechanism are as follows:

Step-1: The confidential information is encrypted using symmetric key.

Step-2: Noise guided stegging technique is employed

Step-3: Three unlike pixels sets of the binding image are obtained for engrafting.

Step-4: Adaptive K- bit engrafting technique builds different binary pattern for concealment.

Step-1 furnishes a cryptic effect for the confidential data before engrafting, which contributes to the first layer of security. Step-2 furnishes a retiring platform for engrafting the information. Step-3 contributes to choosing the pixels sets for engrafting, clandestine data need not to be engrafted in all the pixels sets, thus increasing the protection. Step-4 extends to furnish unlike binary pattern for apiece pixel sets, it guarantees that hacking the data is unimaginable.

VII. Conclusion

The noise guided stegging with adaptive K- bit engrafting techniques enforced in this paper employing an intelligent helter-skelter engrafting process for the encrypted clandestine data. From the computed results of the concealing capacity of the stego image generated by the proposed method, it is noticed that the adaptive K- bit engrafting techniques supplants the existing techniques in meliorating the concealing capacity of the stego image. 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. This facilitates the system more user friendly. Moreover the noise employed in the proposed technique is random; it leads the classification of pixel sets and its positions in the binding image are unpredictable.

ACKNOWLEDGMENT

Authors wish to thank Mrs. Devipriya silambarasan/ PG Scholar/ SASTRA University for her time, linguistic & technical support.

REFERENCES

[1] “*Digital image steganography: Survey and analysis of current methods*” Abbas Cheddad, JoanCondell, KevinCurran, PaulMcKevitt, *journal of signal processing*

[2] “*Exploring steganography: seeing the unseen*”, N.F.Johnson, S.Jajodia, IEEE Computer 31 (2) (1998) 26–34.

[3] “*Steganography: past, present, future*”. J.C.Judge, SANS Institute publication, <http: // www.sans.org/reading room/ whitepapers/ stenganography/ 552.php>, 2001

[4] “*Hide and seek: an introduction to steganography*”, N.Provos, P.Honeyman, IEEE Security and Privacy 1(3) (2003) 32–44.

[5] “*Data-hiding codes*”, P.Moulin, R.Koetter, Proceedings of the IEEE 93 (12) (2005) 2083–2126.

[6] “*Cryptography: current status and future trends*”, S.B.Sadkhan, in: Proceedings of IEEE International Conference on Information& Communication Technologies: From Theory to Applications, Damascus. Syria, April19–23, 2004, pp.417–418

[7] “Steganalysis using higher-order image statistics”, S.Lyu, H.Farid, IEEE Transactions on Information Forensics and Security 1(1) (2006)111–119.

[8] “*The code breakers: the comprehensive history of secret communication from ancient times to the Internet*”, D.Kahn, Scribner, December 5, 1996.

[9] “*Information noyee, information cach*”, J.P.Delahaye, Pour la Science 229 (1996) 142–146 /www.apprendre-en-ligne.net/crypto/stega no/229_142_146.pdfS (in French).

[10] “*The prisoners’ problem and the subliminal channel*”, G.J.Simmons, in: Proceedings of International Conference on Advances in Cryptology, CRYPTO83, August22–24, 1984, pp.51–67.

[11] “*A cautionary note on image down grading*”, C.Kurak, J.McHugh, in: Proceedings of the IEEE 8th Annual Computer Security Applications Conference, 30 November–4 December, 1992, pp 153-159.

[13] “*Discovering hidden evidence*”, C.Hosmer, Journal of Digital Forensic Practice (1)(2006)47–56.

[14] “*Applications for data hiding*”, W.Bender, W.Butera, D.Gruhl, R.Hwang, F.J.Paiz, S.Pogreb, IBM Systems Journal 39 (3&4) (2000) 547–568.

[15] “*Introduction to information hiding*”, F.A.P.Petitcolas, in: S.Katzen beisser, F.A.P. Petitcolas (Eds.), Information Hiding

[12] “*Alqaeda and the internet: the danger of ‘‘cyber planning’’, parameters*”, T.L.Thomas, US Army War College Quarterly-Spring2003. Available from: www.carlisle.army.mil/usawc/Parameters/03spring/ thomas.pdf .

Techniques for Steganography and Digital Watermarking, Artech House, Inc., Norwood, 2000.

[16] “*A secure data hiding technique with heterogeneous data-combining capability for electronic patient records*”, S.Miaou, C.Hsu, Y.Tsai, H.Chao, in: Proceedings of the IEEE 22nd Annual EMBS International Conference, Chicago, USA, July23–28, 2000, pp. 280–283.

[17] “*Water marking medical images with patient information*”, U.C.Nirinjan, D.Anand, in: Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Hong Kong,China,29October–1November1998,pp.703–706.

[18] “*Protection of mammograms using blind steganography and water marking*”, Y.Li, C.Li, C.Wei, in: Proceedings of the IEEE International Symposium on Information Assurance and Security, 2007, pp.496–499.

[19] “*Using extended file information (EXIF) file headers in digital evidence analysis*”, P.Alvarez, International Journal of Digital Evidence, Economic Crime Institute (ECI) 2 (3) (2004) 1–5

[20] “*A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution*”- M.B. Ould MEDENI, 978-1-61284-732-0/11/$26.00, 2010 IEEE.

[21] “*A New Approach for LSB Based Image Steganography using Secret Key*”- S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain in: Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 2011)

[22] “*A more secure steganography based on adaptive pixel-value differencing scheme*”-Weiqi Luo · Fangjun Huang · Jiwu Huang, Springer Science+Business Media, LLC 2010.

[23] “*A Novel Keyless Algorithm for Steganography*”- Supriya Rai and Ruchi Dubey, in: IEEE proceedings 2012.

[24] “*Who decides hiding capacity? I, the Pixel Intensity*”- Rengarajan Amirtharajan, K.Ramkrishnan, M.Vivek Krishna, Nandhini.J and John Bosco Balaguru Rayappan, in: IEEE proceedings 2012.

[25] “*An intelligent chaotic embedding approach to enhance stego-image Quality*”- Rengarajan Amirtharajan, John Bosco Balaguru Rayappan- Journal of information science.

[26] “*Space-Filling Curves*”, Hans Sagan, Springer- Verlag, New York, 1994. ISBN: 0-387-94265-3.

[27] “*A. Westfeld Space filling curves in steganalysis*”, in: E.J. Delp, III, P.W. Wong (Eds), Security, Steganography and Watermarking of Multimedia Contents VII SPIE 5681, 2005, pp. 28–37.

[28] “*Information secured by the guidance of salt & pepper noise*”-Jayaseelan. J, Kruthika. B- 2013 IEEE International Conference on Computational Intelligence & Computing Research.