EasyChair Preprint

№ 2345

Chaos Encrypted Images on Lossless and Reversible Data Hiding using Wavelet Transform

Konduru Upendra Raju and N Amutha Prabha

January 9, 2020

Chaos Encrypted Images on Lossless and Reversible Data Hiding using Wavelet Transform

K. Upendra Raju [1], Dr. N. Amutha Prabha [2]
[1] Research Scholar, SENSE, VIT, Vellore, India,
Associate Professor, ECE, SVCE, Tirupati – 517507, kupendraraju@gmail.com
[2]Associate Professor, School of Electrical Engineering, VIT University, Vellore, India
amuthaprabha@vit.ac.in

Abstract. Steganography is a process of secret writing or covered writing. This method is implemented to hide information in a protected medium for covered/secret communication. In this process, images will be used as the protected medium for hiding secret data. In this paper an enhanced method of transferring secret data through encrypted images has been implemented. Where, histograms of images are evaluated to detect the types of images for different capacity. Then, DWT algorithm is applied for the grey-scale images to improve the performance. Chaos method is used to encrypt the secret data before embedding the data in lossless and Reversible Data Hiding (RDH) into the protected image and it is encrypted by using encryption key. The images are fused before embedding the encrypted data, and then by using LSB replacement algorithm the data is inserted in the pixels of fused image. For the extraction of secret data a decryption key and IDWT is used to recover the original cover. In this enhanced method, a covered double image is implemented for security problem.

Keywords: Steganography, Encryption, Reversible Data Hiding and Reversible Data Hiding in Encrypted Domain, DWT.

1 Introduction

Image processing is the method of performing visual appearance operations of images and processing the images for analyzing the structures and features present. Generally, scientific images produce information to communicate results, instead of creating an audible tone. In this particular domain the latest enhancement is storing huge amount of data in images and in the meantime it should provide high security. In this proposed method, a combination of steganography and cryptography is implemented. Where, Steganography [1-3] means secret drawing and cryptography is technique of transforming information to secure format and invulnerable to attack. By implementing these two methods, we are going to transfer the data to the destination securely. A Lossless data hiding method is defined as to extract the original text data from the embedded data without any loss of information in the image. In Reversible Data Hiding (RDH) method, if a noise has been added in embedded data, the original cover can be recovered perfectly in the extraction process. The other techniques to

develop the RDH in digital images are RDH in Histogram, RDH in JPEG images, Robust RDH, RDH in contrast Enhancement and RDH in encrypted domain. Literature review pronounces the need for growing application of RDH [4] in image authentication processing, medical image processing. RDH technique is used to recover the embedded message from the original cover without loss by using Public-key Cryptography [5]. In RDH method reconstruction of the embedded secret data is possible as compared to steganography. Reversible data hiding was initially introduced and implemented by [6] to implant secret data in an image by enhancing the PSNR and decreasing the MSE. Chandramouli et al [7] has done Steganalysis to find the embedded data. Steganalysis method is used to recognize the hidden information in a cover image using histogram feature coding technique that detects the existence of stego data.

In the recent years, the combination of encryption and data hiding techniques has been used. In some papers, a simple embedding algorithm was used in data hiding [8]. Encryption techniques are to convert plain text into cipher text by using encryption algorithms. In both the techniques the privacy is low. So to increase the security level of embedded data a combination of both data hiding and encryption techniques are used. In receiver, the authorized user can extract the original text from the cover image. This method is known as Reversible Data Hiding in Encrypted Images (RDHEI) [9]. A RDH in encrypted image is to improve the severity of the security barrier. The performance of RDHEI can be further increased by implementing the order [10] or flipping ratio [11].

A double image encryption method is considered in this paper to transfer the cover data using DWT and chaos algorithm. Two grey scale images are combined using DWT method. Thereafter, by converting the plain text into the binary values, the secret data is embedded in the image. These binary values will be stored in last two bit of Least Significant Bit (LSB). By storing the information in the last two bit of LSB enhance the security of the information and also increase the PSNR value. These particular techniques are widely used in Defense Field, Biomedical field, Multimedia Security and Data Communication. Initially, the first bit of data is extracted from the LSB of the initial high frequency co-efficient and then the second bit of data is extracted from the second coefficients and so on. This process will repeat until all secret data bits are recovered and these bits are grouped into 8-bits to form a character value. Logical bitwise operators like ‘bit and’ and ‘bit or’ are used to extract the desired number of bits. Finally, chaos decryption methodology with specific keys is applied to extract the complete message characters. To compare the values of secret data and threshold value again Chaos algorithm is used to attain the best performance.

In Discrete Cosine Transform (DCT) only vertical and horizontal dimensions are used to hide the data. Hence it is replaced by Discrete Wavelet Transform (DWT). In the DWT the sub bands like LL, LH, HL, and HH are considered to get the clear fused image [12]. By implementing this concept, the fusing technique will provide efficient results compared to other techniques. However, LSB replacement technique has been used in the existing systems. But in this technique, LSB replacement method is implemented along with DWT fusing method. Chaos encryption and decryption algorithm consumes less time as compared to the other techniques which has the ability to compare the secret data and threshold values XOR technique. Also, by implementing the fusing technique the PSNR (Peak Signal to Noise Ratio) will

increase and MSE (Mean Square Error) will reduce as compared to the other existing method [5].

2 Existing Method

In the existing system a lossless data hiding schemes were used for public-key-crypto systems such as Paillier [13] and Damgard - Jarik cryptosystems [14]. In Paillier cryptosystem [13], the public key is composed of 'n' and a randomly selected integer 'g' and the private key is composed as λ, where $n = p.q$, p and q are the prime numbers and $\lambda = lcm\ (p-1,\ q-1)$. In the reverse process of Paillier decryption, the plaintext value can be obtained from the cipher text value by using private key. The data was hidden in encrypted image by using Wet Paper Channel (WPC) [15] in the data embedding process. One may extract the embedded data from the LSB-layer using wet paper coding, if the receiver knows the data hiding key. In [18] Hybrid firefly algorithm was used to embed the data in lossless and RDH in encrypted domain.

In RDH scheme public-key encrypted images are used. In reversible schemes first apply the histogram shrink to the input image. Then apply additive homomorphic cryptosystem to the encryption of each pixel. In the encrypted image, the data hider changes the cipher text pixel values to embed a bit-sequence generated from the additional data and error correction codes. By homomorphic property, there is a change in the encrypted domain which results a change on plain text pixel values. The original plain text image can be retrieved perfectly at the receiver without any overflow/underflow in the decrypted image, since histogram shrink was used before encryption. In the existing methods, used a combination of lossless and RDH using public key encryption. In these two schemes the data were embedding in the encrypted domain using Paillier cryptosystem and Damgard - Jarik cryptosystem. In the reconstruction of data, the above two methods are different. In the lossless scheme, the data extraction from encrypted image has no effect. In the reversible method, a small distortion occurs in the data extraction from the decrypted image. So, the data cannot be extracted in lossless scheme after decryption and the data cannot be extracted in reversible before encryption. The lossless and reversible schemes are shown in fig.1.

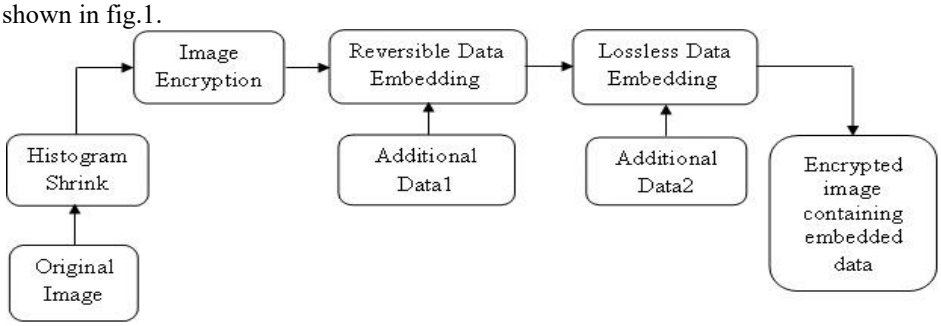

Fig. 1 Sketch of the Lossless and Reversible Data Hiding scheme

3 Proposed Method

From the section - 2, a lossless and reversible data hiding schemes for chaos based encryption using wavelet transform is proposed. In the existing method Data embedding on encrypted domain may result in a slight distortion in plaintext domain due to the homo-morphic property, the embedded data can be extracted and the original content can be recovered from the directly decrypted image and the public key encryption has low efficiency, when image size is very large. To overcome this problem, the objective of this paper is to use the chaos-based image encryption which is an efficient way to deal with the intractable problem of fast and highly secure image encryption. Chaotic systems have many important properties, like the sensitive dependence on initial conditions, system parameters, pseudorandom, non periodicity and topological transitivity property etc. Some of the properties meet the requirements such as diffusion and mixing in the sense of cryptography [16]. Therefore, chaotic based cryptosystems have more advantage in practical applications. The proposed method of chaos based encryption on lossless and reversible data hiding by using wavelet transform of data embedding and extraction process as shown in fig.2 and fig.3.

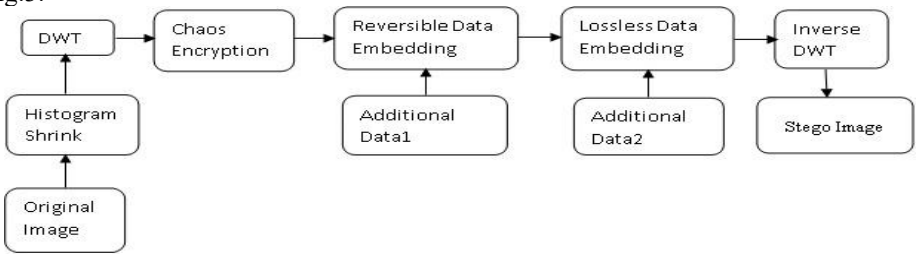

Fig.2 Proposed method of Data Embedding Process

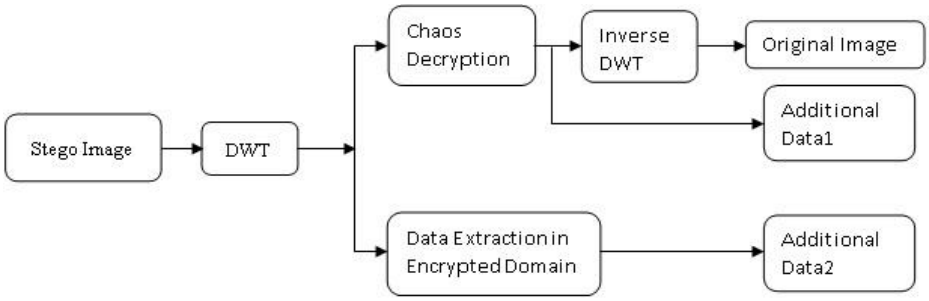

Fig.3 Proposed method of Data Extraction Process

(a) Lena (b) Man (c) Plane (d) Crowd

Fig.4 Cover Images

In the proposed method, the cover image is a Lena image and applies histogram shrinking process by using equation (1). The histogram of an image can be altered by using mapping functions, which will stretch, compress (shrink), or slide the histogram. Histogram shrink is the opposite of a histogram stretch, where image contrast being decreased by reducing the gray levels.

$$Shrink(I_{x,y}) = \left[\frac{Shrink_{max} - Shrink_{min}}{I_{x,y(max)} - I_{x,y(min)}}\right](I_{x,y} - I_{x,y(min)} + Shrink_{min}) \quad (1)$$

After applying histogram shrink, convert spatial domain image into frequency domain by applying DWT. Wavelets are very popular in image processing, denoising and compressions. Haar wavelet transform were used in the proposed method to transform the image. Chaos encryption technique is an advanced encryption technique which can be used to encrypt the image or text for secure transmission of information. In this technique, select chaotic keys (u, x) and compare the length of the transformed image size. If the value is less than the size of the image, then generate encrypted threshold value. The original DWT Image encrypts with encryption key value which is created from chaotic process with a threshold value by 'BITXOR' operation. A logistic map is implemented for simulation of chaotic map sequence. It is very efficient to transmit the secret data through an unsecure medium securely which avert hacking the secured information [11]. Chaotic sequence can be defined on a real or complex number space known as boundary continuous space. The flow chart of Chao's image encryption as shown in fig. 5. After chaotic encryption, apply lossless and RDH techniques mentioned in section-II. To recover the original encrypted image, by apply inverse discrete wavelet transform as shown in fig.2

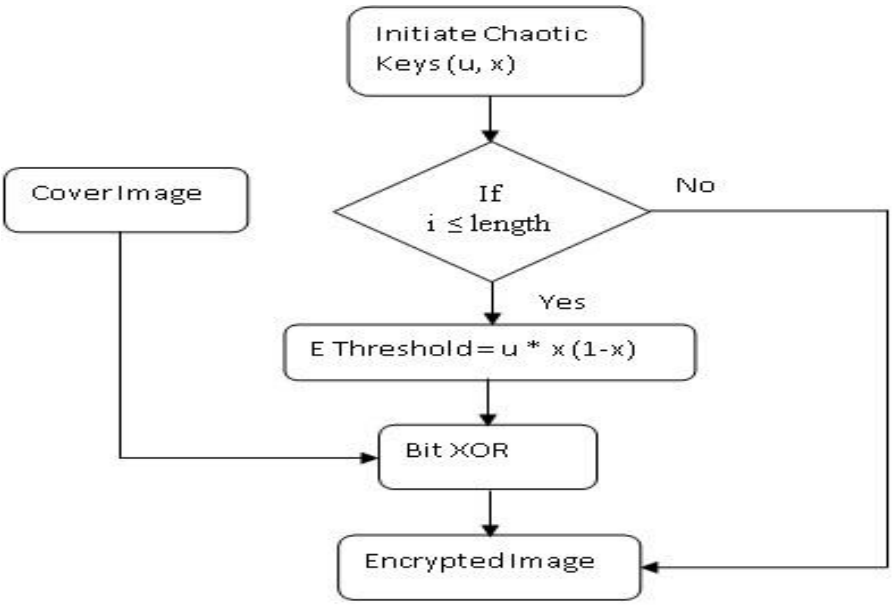

Fig. 5 Chao's Encryption Flow Chart

At the receiver, the stego image consists of original image and secret data. The DWT was applied before extraction of original data from the cover image. The additional data-2 can be extracted by directly decrypting the stego image in lossless. Apply the chaotic decryption algorithm for extraction of additional data-1and to process the transformed image by IDWT to recover the original cover image perfectly without loss.

4 Experimental Results

Four gray images sized 512 × 512, Lena, Plane, Man, and Crowd shown in Figure.4 is used as original plaintext in this paper. Using Chaos cryptosystem, all the pixels in the cover image were initially encrypted with the implementation of lossless scheme. By using Lossless and reversible data hiding schemes, additional data were embedded into cipher-text pixel values of LSB-planes. The comparison rate of PSNR performance between the proposed lossless and reversible scheme and existing methods with different (δ=0, 4 and 7) values are stated in Table-I.

Table-I

PSNR Analysis of Proposed System (Delta=0)				
Emb Cap/ Image	**Lena**	**Man**	**Plane**	**Crowd**
0	77.6624	77.618	78.7559	77.545
0.05	63.9422	63.9076	63.9675	63.8565
0.1	61.0849	61.0435	61.0248	61.0686
0.15	59.3213	59.2977	59.3242	59.3042
0.2	58.0435	58.0667	58.1007	58.1084
0.25	57.0948	57.1154	57.1366	57.1111

PSNR Analysis of Proposed System (Delta=4)				
Emb Cap/ Image	**Lena**	**Man**	**Plane**	**Crowd**
0	53.1636	53.0943	53.1417	53.1125
0.05	52.8778	52.8127	52.8854	52.8637
0.1	52.6118	52.5451	52.6172	52.6059
0.15	52.3751	52.2883	52.353	52.3621
0.2	52.1374	52.0849	52.1326	52.1528
0.25	51.9018	51.8799	51.9043	51.9176

PSNR Analysis of Proposed System (Delta=7)				
Emb Cap/ Image	**Lena**	**Man**	**Plane**	**Crowd**
0	53.1388	53.0614	53.1243	53.0599
0.05	37.6461	37.2659	36.455	36.6639
0.1	34.8882	35.0913	33.839	33.6188
0.15	32.6672	33.0027	32.5154	32.3749
0.2	30.9253	31.2453	31.255	31.1698
0.25	30.5612	30.7034	30.3862	30.6198

With a larger value of δ, a higher embedding capacity could be ensured, while a higher distortion would be introduced into the directly decrypted image. For instance, when using Lena as the cover and δ=4, a total of 4.6×10^4 bits were embedded and the value of PSNR in directly decrypted image was 40.3 dB in existing method and 52.37dB in the proposed method. When using δ = 7, a total of 7.7×10^4 bits were embedded and the value of PSNR in directly decrypted image was 36.3 dB in existing method and 37.64dB in the proposed method. The proposed method yields better performance by the inclusion of DWT before encryption.

The fig. 6 shows the performance curves for proposed lossless and reversible data hiding in encrypted domain scheme of four test images Lena, Man, Plane, and Crowd at δ = 0. It produces the PSNR value with different embedding capacity. The PSNR reduces while increasing the embedding rate.

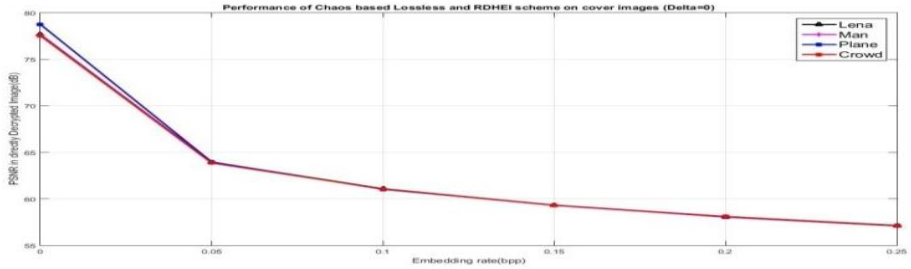

Fig. 6 Performance of Chaos based encryption on cover images at δ=0

The fig. 7 displays the performance of PSNR Vs Embedding rate of different cover images at δ=4. From the graph, Lena image gives highest PSNR than other image for different embedding rates

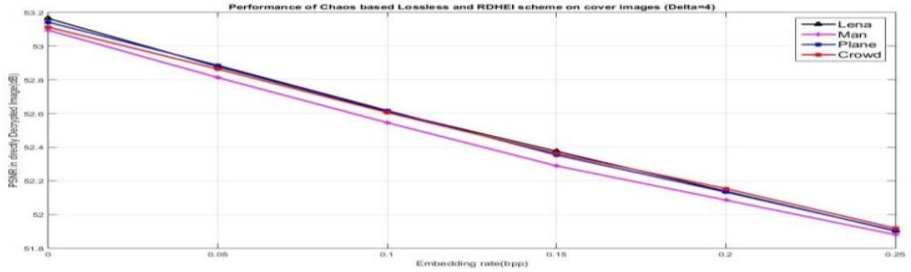

Fig. 7 Performance of Chaos based encryption on cover images at δ=4

The fig.8 explain the performance criteria of different images with embedding capacity at δ=7. Lena images give the better performance than the other images for different embedding rates.

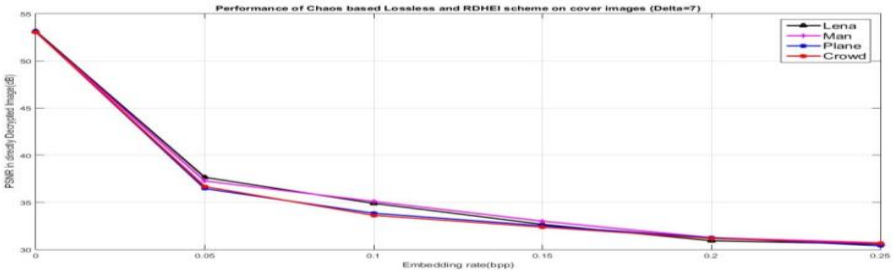

Fig. 8 Performance of Chaos based encryption on cover images at δ=7

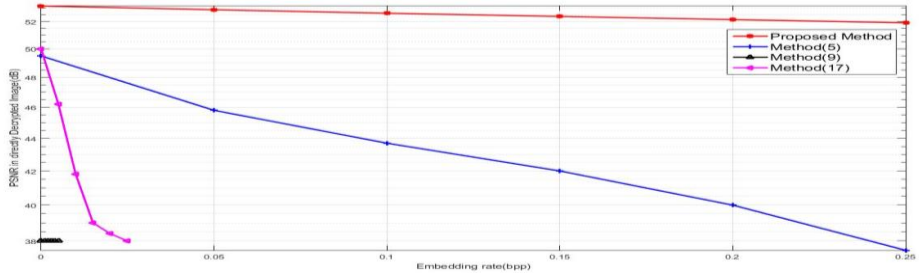

Fig.9 Comparison of Embedding rate Vs PSNR performance between the proposed scheme and previous method

The embedded additional data and the original plaintext image were extracted and recovered without any error. The fig.9. Shows the embedding capacity rate Vs PSNR performance between the proposed method and existing methods [5], [9] and [17] of Lena image at a constant values of δ = 4 under the condition of successful data extraction/image recovery. In [9] and [17], the block of encrypted image is to carry only one additional bit. Therefore, the embedding rates are fixed and PSNR value is low. In [5], used combination of lossless and RDH in public key encryption such as Paillier and Damgard-Jurik cryptosystems. In [5], the image was encrypted for the entire image. The key was public, high computational complexity and security level is low. In the proposed system, chaos encryption and DWT method are implemented, the image was encrypted only LL band and the data was embedded in the DWT image only. Therefore, the computational complexity reduces and the PSNR increases as shown in fig.9.

The Table - II shows the performance parameters of Lena image with different embedding rates and different delta values. From the analysis made in Table-I, Lena image is selected as cover image, since it gives better performance compared to other images with respect to embedding capacity and δ values of equal size. The performance metrics are Mean Square Error (MSE), PSNR, Correlation, Structural Similarity Index (SSIM) gives the perceptual quality of degraded image and Universal Image Quality Index(UIQI) used as quality distortion measure with a value range of [0, 1] gives how close the mean luminance between two images. From the Table-II, PSNR value is high due to DWT transform and MSE is low. Since, MSE and PSNR are inversely proportional. The correlation and SSIM values indicate that the cover

image was perfectly reconstructed with different embedding capacity and δ values. The luminance value of Lena image in the proposed method is approximately equal to the theoretical value (=1) at δ = 0. At δ=4 and 7 the luminance value is reduced due to shrinking factor.

Performance of Proposed method of Lena Image				
Embedding Capacity	**Image Parameter**	**Delta = 0**	**Delta = 4**	**Delta = 7**
0	**MSE**	0.0011	0.3138	0.3156
	PSNR	77.6624	53.1636	53.1388
	Correlation	1	0.9999	0.9999
	SSIM	1	0.9869	0.9871
	UIQI	0.9991	0.6986	0.6966
0.01	**MSE**	0.0059	0.3179	11.1806
	PSNR	70.3961	53.1085	37.6461
	Correlation	1	0.9999	0.9968
	SSIM	0.9999	0.9869	0.9426
	UIQI	0.9963	0.6985	0.6765
0.05	**MSE**	0.0262	0.3352	11.1806
	PSNR	63.9422	52.8778	37.6461
	Correlation	1	0.9999	0.9968
	SSIM	0.9997	0.987	0.9426
	UIQI	0.9624	0.6984	0.6765
0.1	**MSE**	0.0507	0.3564	21.099
	PSNR	61.0849	52.6118	34.8882
	Correlation	1	0.9999	0.9939
	SSIM	0.9994	0.9871	0.9117
	UIQI	0.9504	0.6982	0.6491
0.15	**MSE**	0.076	0.3763	35.1852
	PSNR	59.3213	52.3751	32.6672
	Correlation	1	0.9999	0.9899
	SSIM	0.9989	0.9873	0.8413
	UIQI	0.8589	0.697	0.6198
0.2	**MSE**	0.102	0.3975	52.5471
	PSNR	58.0435	52.1374	30.9253
	Correlation	1	0.9999	0.9851
	SSIM	0.9985	0.9875	0.7769
	UIQI	0.7801	0.6962	0.6013
0.25	**MSE**	0.1269	0.4197	57.1429
	PSNR	57.0948	51.9018	30.5612
	Correlation	1	0.9999	0.9839
	SSIM	0.998	0.9877	0.7251
	UIQI	0.7033	0.6959	0.5902

5 Conclusion

This paper proposed the implementation of chaos based encryption and DWT transformation technique and compared with existing methods of lossless and RDH technique. The proposed method gives better performance with various cover images and different embedding capacity with different δ values. Finally, Lena image is considered as cover image and measured the different performance parameters are compared. The graphs and tables state that the proposed techniques outperforms with less complexity, higher efficiency.

References

1. 1. J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge, U.K.: Cambridge Univ. Press, 2009.
2. T. Morkel , J.H.P. Eloff and M.S. Olivier "*An Overview of Image Steganography*".
3. N. Provos and P. Honeyman, Hide and seek: "An introduction to steganography," *IEEE Security and Privacy*, 01 (3) (2003) page no 32-44.
4. K. Upendra Raju, N.Amutha Prabha "A Review of Reversible Data Hiding technique based on Steganography", *Proceedings of ARPN Journal of Engineering and Applied Science*, vol.13, No.3, page no.1105-1114, Feb.2018, ISSN.1819-6608
5. X.Zhang, J.Long, Z.Wang and H.Cheng "Lossless and Reversible Data Hiding in Encrypted Images with Public-Key Cryptography", *IEEE Transactions on circuits and Systems for Video Technology*, vol.26, No.9, page no.1622-1631, Sept.2016.
6. Y. Q. Shi, "Reversible data hiding", in *Proc. Int. Workshop Digit.Watermarking*, 2004, page no. 1-12.
7. R. Chandramouli, M. Kharrazi, N. Memon, "Image Steganography and Steganalysis: Concepts and Practice" *International Workshop on Digital Watermarking*, Seoul, October 2004.
8. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding", *IEEE Trans. Image Process.*, vol. 14, no. 2, page no. 253 - 266, Feb. 2005.
9. X.Zhang, "Reversible data hiding in encrypted images", *IEEE Signal Process, Lett.,* vol. 18, no. 4, pp. 255-258, Apr. 2011.
10. W.Hong, T,-S Chen, and H,-Y. Wu, "An Improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Lett.* vol. 19, no. 4, pp.199-202, Apr. 2012.
11. J. Yu, G.Zhu, X. Li, and J.Yang, "An improved algorithm for reversible data hiding in encrypted images," in *Proc. 11th Int. workshop Digit. Forensics Watermarking (IWDW),* vol. 7809. Shanghai, China, Oct./Nov. 2012, pp. 358-367

12. EsamHagras A, El-Mahallawy M.S, ZeinEldin A and Fakhr M.W, "Robust Secure and Blind Watermarking Based On DWT DCT Partial Multi Map Chaotic Encryption," *International Journal of Multimedia and Its Application*, 3 (4), 2011.
13. P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 1592, Berlin, Germany: Springer-Verlag, 1999, pp.223-238.
14. I.Damgard and M.Jurik, "A generalization, a simplification and some applications of paillier's probabilistic public-key system," in *Public Key Cryptography,* Berlin, Germany: Springer-Verlag, 2001, pp. 119-136.
15. J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper," *IEEE trans. Signal Process.,* vol. 53, no. 10, pp. 3923-3935, Oct. 2005.
16. Zhang LH, Liao XF, Wang XB. An image encryption approach based on chaotic maps. Chaos, Solitons & Fractals 2005; 24: 759–65.
17. X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security,* vol. 7, no. 2, pp. 826-832, Apr. 2012.
18. K. Upendra Raju, N.Amutha Prabha "Improved Data Security using Lossless and Reversible Data Hiding Technique in Encrypted Images with Hybrid Firefly Algorithm", *Proceedings of Journal of Advanced Research in Dynamical & Control System*, vol.11, No.8, page no.163-171, 2019, ISSN.1943-023X