

Reversible data embedding using wavelet technique and lossless recovery of original images

¹Iakshmi Narayanan.S,

¹ Asst.Prof / ECE, Sri Ramakrishna Engineering College,

²Dr. Sankaranarayanan.K, Dean,

² Sri Ramakrishna Institute Of Technology,

³ Dr. Vijayakumari. V, Prof/ECE,

³ Sri Krishna College Of Technology,

⁴Keerthana.S, ⁵Haripriya.N, ⁶JasmineNiketha.M,

Sri Ramakrishna engineering college, Coimbatore, Tamilnadu.

ABSTRACT

Steganalysis of image and text is done by the use of Reversible watermarking and Lossless Data hiding techniques respectively. Reversible watermarking is a special watermarking technique which allows to extract both the hidden image and the exact original image from the watermarked content by the use of DWT coefficients. Reversible data hiding (RDH), the original cover can be restored without losses after the embedded information is extracted by histogram shift (HS) method. In RDH, CA is used for encryption and decryption of a cipher text. The Discrete wavelet transform is more efficient at higher threshold values. Here we improve PSNR, MSE values and the extracted image will have the same image quality and resolution.

INDEX TERMS— Reversible watermarking, Reversible data hiding, Histogram Shifting, Steganography.

I. INTRODUCTION

Steganography is a data hiding methodology which enables clandestine and secure communication in a statistically undetectable way. Using such techniques innocuous digital assets such as audio, image and video can be used as covert communication channels. The word "Steganography" is of Greek origin and means "covered or hidden writing". The main aim in steganography is to hide the very existence of the message in the cover medium. Steganography is a branch of hidden information science, which tries to achieve an ideal security level in military and commercial usages, so that sending the invisible information will not be exposed or distinguished by the others. Steganography is implemented in frequency domains [1]. The RGB color model is an additive color model in which red, green and blue light are added together in various ways to reproduce a broad array of colors. RGB value does not define the same color across devices without some kind of color management. Chrominance is the signal used in video systems to convey the color information of the picture, separately from the accompanying luma signal. Chrominance is usually represented as two color-difference components: $U = B' - Y'$ (blue - luma) and $V = R' - Y'$ (red - luma). In composite video signals, the U and V signals modulate a color subcarrier signal, and the result is referred to as the chrominance signal; the phase and amplitude of this modulated chrominance signal correspond approximately to the hue and saturation of the colour.

Luminance is invariant in geometric optics i.e., for an ideal optical system, the luminance at the output is the same as the input luminance and the output luminance is at most equal to the input. For example, if we form a demagnified image with a lens, the luminous power is concentrated into a smaller area, thus the luminance is higher at the image. The light at the image plane, however, fills a larger solid angle; the luminance comes out to be the same assuming there is no loss at the lens. The image can never be "brighter" than the source. Luminance is often used to characterize emission or reflection from flat, diffuse surfaces. Losses will be more in RGB color model so Chroma and luma bands are used.

II. PREVIOUS WORK

A novel DCT domain Steganalysis method is proposed in which the features derived from multivariate p.d.f.s calculated with MRF cliques from the DCT coefficients are considered. The simulation results showed that in general the proposed steganalyzers perform better compared to the current state of the art. SVM classifiers are used for classification and they analyze and recognize patterns or data[1]. The basic idea is to consider higher dimensional probability distributions in Steganalysis and to increase the secret communication rate, i.e., the embedding rate. In this section, we used multivariate p.d.f. estimates along with MRF cliques. In the literature, some examples of successful Steganalysis algorithms which attack on a univariate p.d.f preserving stego systems have been already shown on DCT domains. In order to take the detection performance, we need to consider correlated random variables (r.v.s) and Markov Random Fields (MRFs). If a random field satisfies the positivity and the Markovianity properties it is called a Markov Random Field.

Once we determine the neighboring system for MRF cliques, the next step is to construct K-variate p.d.f.s. In order to take into account correlations among the neighboring DCT coefficients, along with the original DCT domain (org), we considered horizontal (hor), vertical (ver) and zigzag (zig) scanning schemes for 8x8 blocks. In the modern steganography the sign of the coefficients is not changed, therefore only the absolute value of the coefficients is considered in this work. In order to reduce the dynamic range and to get rid of the variable feature size from one image to other, we set a threshold $T=10$ so that all the coefficients above T are rounded to T [11]. When steganography considers $T>10$ it cannot embed high rates, which yields high power of embedding noise and high detectability.

The embedding procedure covers F5, JPEG Hide & Seek, MB1, MB2, and Outguess, nsF5, MMEEx and YASS methods. For F5, Outguess, MMEEx [3] and YASS [1], we consider the compressed images with the same quality factor used to obtain the stego images as cover images in order not to detect the compression but the pure embedding noise. 0.4, 0.2, 0.1, 0.05 embedding rates (bit per nonzero DCT coefficients) are considered with exceptions applied to Outguess and MB2. 0.4 rate is discarded for these two methods because the embedding operation could not be established for many images in the image set. NsF5 algorithm is obtained from and uses the same quality matrix of the input image for embedding.

Low embedding distortion provided by the MMEEx algorithm is mainly due to the matrix embedding strategy. In order to be able to embed 0.4 rate to all of the images in the image set, one needs to consider (1, 7, 3) or lower coding rates which also makes the experiments comparable to F5 algorithm. We call the MME2 algorithm which uses (1, 7, 3) code as MME2-(1, 7, 3) throughout the paper. Note that lower code rates introduce higher distortion which we avoid to have in the experiments. An SVM classifier is used in all experiments because it has strong regularization properties which help the generalization of the model to an incoming (test) data. The parameters of the SVM classifier are conveyed to the following training and testing phases. We train the classifiers using 20,000 images which are randomly chosen from Memon image set. For each quality, equal numbers of images are considered from each embedding rate for all steganography methods. The training set contains images equally from various qualities (low, medium and high) and rates, 0.4, 0.2, 0.1 and 0.05. The rest of the images are used for testing. The images in the training and testing sets never overlap. We chose Memon image set deliberately because our aim is to design a classifier as robust as possible in terms of different conditions encountered in the real world. A detector which is trained for the worst conditions, i.e., for any possible deviations from the chosen model, can never perform worse than the training conditions. By taking into account the diversity of Memon image set, we consider it as an uncontrolled environment and, therefore, our classifiers are trained and tested by features derived from this set. Memon image set may contain some images which already have secret messages and using them as cover would decrease the performance of the Steganalysis. Goljan set is considered as a controlled environment because the source of the images is known and the general content of the images in this set is completely natural. The classifiers trained in the Memon set are also tested in Goljan set to present the cover-source mismatch problem which has not been well covered in the steganalysis research field. Cover-source mismatch refers to the performance, which occurs if the classifier used is trained on an image set but it is tested in a different one.

Comparative study of DCT and DWT: The performance of DCT is almost similar to DWT at low threshold values but for higher thresholds DWT gives better visual image quality than DCT. At higher threshold values, DWT provides better image quality than DCT. For higher threshold values DCT cannot be used because of poor image quality [10].

III. PROPOSED EMBEDDING TECHNIQUES

A.DWT DOMAIN STEGANALYSIS:

1).DWT Coefficients: In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency *and* location information (location in time)[7].

2).Haar wavelets: The first DWT was invented by Hungarian mathematician Alfred Haar. For an input represented by a list of 2^n numbers, the Haar wavelet transform may be considered to pair up input values, storing the difference and passing the sum. This process is repeated recursively, pairing up the sums to provide the next scale, which leads to $2^n - 1$ differences and a final sum.

3).One Level of the Transform: The DWT of a signal x is calculated by passing it through a series of filters. First the samples are passed through a low pass filter with impulse response resulting in a convolution of the two:

$$y[n] = (x * g)[n] = \sum_{k=-\infty}^{\infty} x[k]g[n - k] \quad (1)$$

The signal is also decomposed simultaneously using a high-pass filter. The outputs giving the detail coefficients (from the high-pass filter) and approximation coefficients (from the low-pass). It is important that the two filters are related to each other and they are known as a quadrature mirror filter. Since half the frequencies of the signal have now been removed, half the samples can be discarded according to Nyquist's rule. The filter outputs are then subsampled by 2 (Mallat's and the common notation is the opposite, g- high pass and h- low pass):

$$y_{low}[n] = \sum_{k=-\infty}^{\infty} x[k]h[2n - k] \quad (2a)$$

$$y_{high}[n] = \sum_{k=-\infty}^{\infty} x[k]g[2n - k] \quad (2b)$$

This decomposition has halved the time resolution since only half of each filter output characterizes the signal. However, each output has half frequency band of the input so the frequency resolution has been doubled.

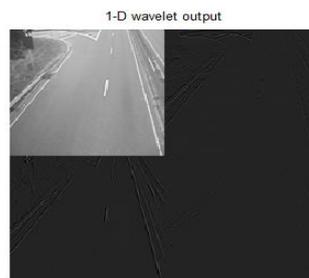


Figure 1: 1-D Wavelet Transform

B.REVERSIBLE WATERMARKING:

The advent of the Internet and the wide availability of computers and printers make digital data exchange and transmission a simple task. A digital watermark is an invisible signature embedded inside an image to show authenticity and ownership. An effective digital watermark should be perceptually invisible to prevent obstruction of the original image. It should be statistically invisible to prevent detection, and it should also be robust to many image manipulations, such as filtering, additive noise, and compression [7]. Digital Watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has been proposed as a new, alternative method to enforce the intellectual property rights and protect digital media from tampering. It involves a process of embedding into a host signal a perceptually transparent digital signature, carrying a message about the Signature is called the digital watermark. The digital

watermark contains data that can be used in various applications, including digital rights management, broadcast monitoring and tamper proofing. Although perceptually transparent, the existence of the watermark is indicated when watermarked media is passed through an appropriate watermark detector. Digital watermarking has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid Proliferation of digital content[8]. Figure 2 represents the process of watermarking technique of an image.



Figure 2: Watermarked Images

C.IMAGE EXTRACTION:

In machine learning, pattern recognition and in image processing, image extraction starts from an initial set of measured data and builds derived values (features) intended to be informative, non-redundant, facilitating the subsequent learning and generalization steps, in some cases leading to better human interpretations. Image extraction is related to dimensionality reduction. When the input data to an algorithm is too large to be processed and it is suspected to be redundant (e.g. the same measurement in both feet and meters, or the repetitiveness of images presented as pixels), then it can be transformed into a reduced set of features (also named features vector). This process is called image extraction. The extracted images are expected to contain the relevant information from the input data, so that the desired task can be performed by using this reduced representation instead of the complete initial data. After embedding process the image is extracted from the cover image which is shown in figure 3.



Figure 3: Extracted Images

D.DATA HIDING:

Data hiding, also called information hiding, plays an important role in information security. It aims at embedding imperceptible confidential information in cover media[8]. The data hiding scheme proposed in this work can be classified into the category of steganography. Here we use Reversible Data Hiding(RDH)[9] for embedding data into images. Chaotic Algorithm is used for encryption and decryption of data.RDH introduces a generalization of the well-known LSB (least significant bit) modification method as the underlying irreversible (lossy) embedding technique. This technique modifies the lowest levels- instead of bit planes- of the host signal to accommodate the payload information. A lossless data embedding algorithm for continuous-tone images is built on the generalized LSB modification method[5]. The reversible data hiding schemes based on histogram shifting were proposed.

In these schemes, peak point in the histogram of the cover image is used to select the embedding area for the secret data, then the part [Peak point +1, Zero point] is shifted to get the embedding area. The chaotic systems are employed in confusion and diffusion stages[12]. Also complex chaotic maps are chosen rather than the simple ones to further enhance the complexity of the algorithm and thereby improving the security. The input to the cryptosystem is the plain image which is to be encrypted. The cryptosystem consists of two stages. The first stage is the confusion stage and the second one is the diffusion stage. The whole confusion-diffusion round repeats for a number of times to achieve a satisfactory level of security[2][12].

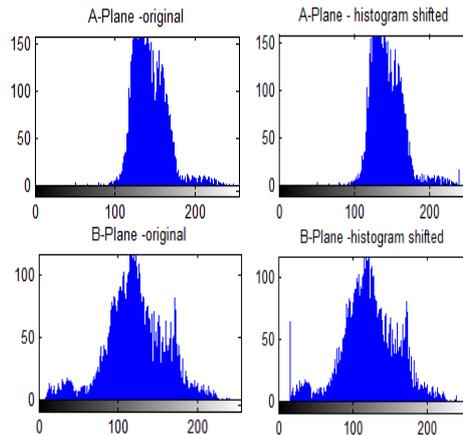


Figure 4: Histogram Shifted Values

E.DATA EXTRACTION:

Data extraction starts from an initial set of measured data and builds derived values (features) intended to be informative, non-redundant, facilitating the subsequent learning and generalization steps, in some cases leading to better human interpretations. Feature extraction is related to dimensionality reduction.

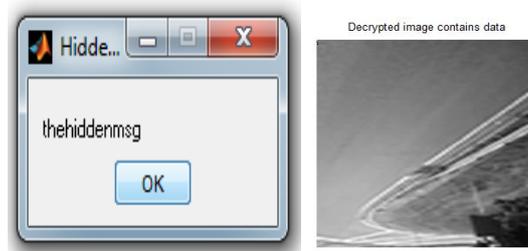


Figure 5: Extracted Text and Decrypted Image

The secret image which is embedded in an image and the decrypted image which contains data is shown in figure 5. When the input data to an algorithm is too large to be processed and it is suspected to be redundant (e.g. the same measurement in both feet and meters, or the repetitiveness of images presented as pixels), then it can be transformed into a reduced set of data (also named data vector). This process is called feature extraction[4]. The extracted features are expected to contain the relevant information from the input data, so that the desired task can be performed by using this reduced representation instead of the complete initial data.

IV. EXPERIMENTAL RESULTS:

As we know steganography includes hiding of an image and is used for security purposes. In the proposed method both the advantages of steganography and cryptography are included. Initially from the input video the required frame is selected and is converted to chrominance and luminance components. Luminance or chrominance components can be used as a cover image. Here we make use of luminance(Y) component. RGB components cannot be used there is a probability of data losses to occur more.

To the Y component 1-level Wavelet transform is applied. Also, Multilevel wavelet transform can be used which improves the image quality. In wavelet transform there are four basic components [LL,LH,HL,HH]. Here we make use of LL component as it retains the original quality of input data where as other components contain more noises and losses can occur while transmission. Wavelet transformations are far better at high compression levels and thus increase the level of robustness of the information that is hidden, something which is essential in an area like watermarking.

The type of embedding process has to be chosen via image or text. If the embedding process is image digital watermarking steganographic method is applied to the secret image. In Watermarking, the extracted image has the same image quality as that of the original image. On the other hand, if the embedding process is text Reversible data hiding (RDH) algorithm is applied. Here encryption and decryption algorithms are used for secured data transmission.

A. EMBEDDING PROCESS:

In this project two input is given one is video clipping of any format other one is secret image to hide. The input video is converted into chrominance and luminance component. The video frame is read using mmreader and is stored as frame in the memory from that particular frame is extracted randomly. To that particular frame, wavelet transform is applied. Based on the hidden information embedding process is selected. Based on the selection of information which is to be hidden the embedding process is chosen. When the information is image, the digital watermarking algorithm is implemented. Performance analysis such as PSNR, MSE, RMSE, and NCC are valuated.

When the information is text, the reversible data hiding (RDH) encryption and decryption algorithms are implemented. For the encryption process to occur a Histogram Shifting (HS) technique is applied, meanwhile, a secret key is generated. In this project output is extracted directly without the use of any classifier or separate algorithms. There are two outputs one is image and the other is data. The output of reversible watermarking is the extracted original image from the hidden image. The image on decryption requests for a password to extract the hidden data, when the same password as encryption is entered hidden data as well as the cover image is separated in reversible data hiding technique.

B. PERFORMANCE ANALYSIS OF AN IMAGE:

i. MSE: The mean-squared error (MSE) has been the dominant quantitative performance metric in the field of signal processing. It remains the standard criterion for the assessment of signal quality and fidelity; it is the method of choice for comparing signal processing methods and systems. Usually, it is assumed that one of the signals is a pristine original, while the other is distorted or contaminated by errors.

MSE is defined as

$$MSE = \frac{1}{m n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \quad (3)$$

ii. PSNR: Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content. The PSNR (in dB) is defined generally as:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX^2}{MSE} \right) = 20 \cdot \log_{10} \left(\frac{MAX}{\sqrt{MSE}} \right) \quad (4)$$

Where $I(i,j)$ is the original image, and $K(i,j)$ is the decompressed image and m,n are the dimensions of the image. Here, MAX is the maximum possible pixel value of the image. Generally, when samples are represented using linear PCM with B bits per sample, MAX is 2^B-1 . For color images with three RGB values per pixel, the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three. Alternately, for color images the image is converted to a different color space and PSNR is reported against each channel of that color space, e.g., YCbCrorHSL[6].

S.NO	PARAMETER	SECRET IMAGE	EXISTING SYSTEM RESULT FOR IMAGE	PROPOSED SYSTEM RESULT FOR IMAGE	PROPOSED SYSTEM RESULT FOR TEXT	
					TEXT	SECRET TEXT
1.	PSNR		61.126	65.298	69.113	PIGEON
	MSE		28.392	17.652	10.156	
2.	PSNR		61.175	65.817	68.106	THEHIDDEN MSG
	MSE		28.489	17.641	2.289	
3.	PSNR		61.096	64.896	75.032	ABC
	MSE		27.279	17.713	3.12	
4.	PSNR		61.521	63.870	74.845	LOGO
	MSE		28.342	17.628	2.865	
5.	PSNR		61.150	63.841	74.983	CHROME
	MSE		28.101	17.595	2.178	
6.	PSNR		61.232	64.992	73.699	SREC
	MSE		28.322	17.606	1.523	
7.	PSNR		61.250	64.463	74.961	ECE
	MSE		26.974	17.639	6.652	
8.	PSNR		61.140	63.834	67.505	YOU ARE THE BEST
	MSE		28.252	17.737	2.234	
9.	PSNR		61.606	65.135	69.926	BUTTERFLY
	MSE		28.171	17.656	2.245	

Table 1: Comparison between PSNR and MSE values of Existing system and Proposed System.

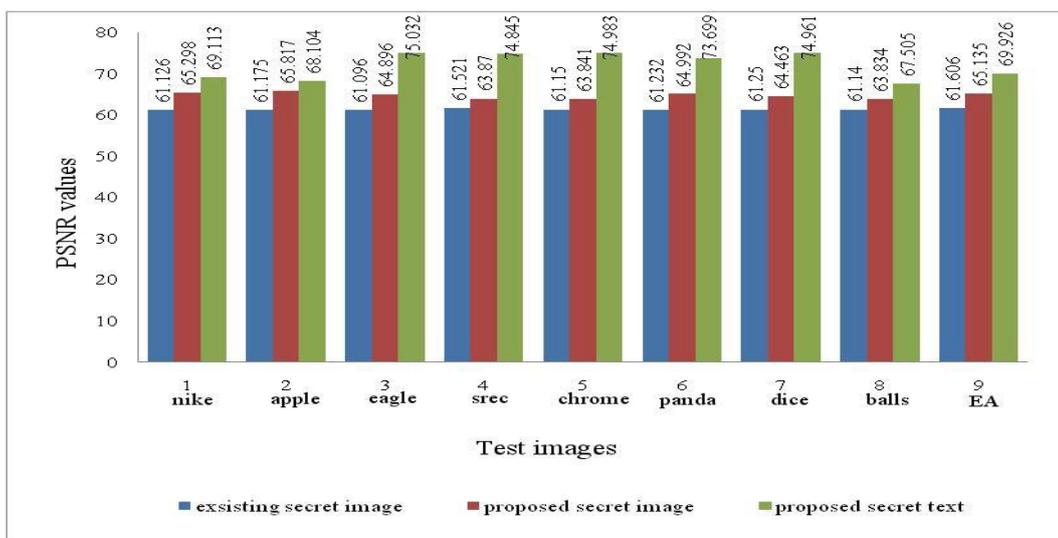


Figure 6: Comparison Of PSNR Values

V. V.CONCLUSION:

In this paper a novel DWT domain steganalysis is proposed. The proposed method has been tested over a wide range of videos with .avi format. The popular hiding techniques such as reversible water marking and reversible data hiding methods are considered for embedding and extraction. Steganalysis can be performed at higher threshold values. RCA algorithm is made use for encryption and decryption and is most effective in parallel processing environment. In our proposed paper we included both watermarking and data hiding for a single video frame. The simulation results showed that in general the proposed design performs better compared to the current state of the art. The problem of security during encryption and extraction occurs. This problem can be mitigated by the use of special characters.

REFERENCES:

- [1] "JPEG Image Steganalysis Using Multivariate PDF Estimates With MRF Cliques" Gökhan Gül, Student Member, IEEE, and Fatih Kurugollu, Senior Member, IEEE Transactions on Information Forensics and Security, Vol.8, No.3, March 2013.
- [2] "Reversible data hiding based on multilevel histogram modification and sequential recovery" Zhenfei Zhao, Hao Luoc,*, Zhe-Ming Luc, Jeng-Shyang Pand, International Journal of Electronics and Communications (AEÜ), Science Direct, Jan 2011.
- [3] "Performance study of common image steganography and steganalysis techniques" Mehdi Kharrazi Husrev T. Sencar Nasir Memon Journal of Electronic Imaging 15(4), 041104 (Oct–Dec 2006).
- [4] "Reversible Data Hiding for High-Quality Images Based on Integer Wavelet Transform" Ching-Yu Yanga Chih-Hung Linband Wu Chih Hua Journal of Information Hiding and Multimedia Signal Processing 2012 ISSN 2073-421 Ubiquitous International Volume 3, Number 2, April 2012.
- [5] "Lossless Data Hiding Using Histogram Shifting Method Based on Integer Wavelets" Guorong Xuan¹, Qiuming Yao¹, Chengyun Yang¹, Jianjiong Gao¹, Peiqi Chai¹, Yun Q. Shi², and Zhicheng Ni². Q. Shi and B. Jeon © Springer-Verlag Berlin Heidelberg 2006.
- [6] "Reversible Data Hiding VIA Optimal Code for Image" Senthil Rani D.#, Gnana Kumari.R International Journal of Modern Engineering Research (IJMER), Vol. 3, Issue. 3, May - June 2013.
- [7] "Secure Data Hiding Technique Using Video Steganography and Watermarking" Shivani Khosla, Paramjeet Kaur International Journal of Computer Applications (0975 – 8887) Volume 95– No.20, June 2014.
- [8] "Steganography and digital watermarking", Copyright © 2004, Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, School of Computer Science, The University of Birmingham.
- [9] "Reversible Data Hiding: Principles, Techniques, and Recent Studies", Masoud Nosrati, Ronak Karimi, Mehdi Hariri World Applied Programming, Vol (2), Issue (5), May 2012 ©2011 WAP journal.
- [10] "Compression analysis between DWT and DCT Introduction" Bhawana Tewari, Sonali Dubey, M. Nizamuddin, Journal of Information Engineering and Applications www.iiste.org ISSN 2224-5758 (print) ISSN 2224-896X (online) Vol 1, No.2, 2011
- [11] Y. Q. Shi, C. Chen, and W. Chen, "A Markov Process Based Approach To Effective Attacking JPEG Steganography," in proc. 8th int. Conf. Information Hiding, j. L. Camenisch, c. S. Collberg, n. F. Johnson, and P. Sallee, eds., 2007, vol. 4437, Incs, springer-verlag.
- [12] "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011, K. Sakthidasan@Sankaran and B. V. Santhosh Krishna.