International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-2 Issue-5, November 2013

Binary Text-Image Steganography

Manisha Boora, Monika Gambhir

Abstract – Unlike encryption, steganography hides the very existence of secret information rather than hiding its meaning only. Image based steganography is the most common system used since digital images are widely used over the Internet and Web. The main aim of steganography is to increase the steganographic capacity and enhance the imperceptibility or undetectability. However, steganographic capacity and imperceptibility are at odds with each other. In addition, there is a tradeoff between both steganographic capacity and stego image quality. Hiding more data in cover images (higher capacity) introduces more artefacts into cover images and then increases the perceptibility of hidden data . Furthermore, it is not possible to simultaneously maximize the security and capacity of a steganographic system. Therefore, increasing steganographic capacity and enhancing stego image quality are still challenges. Secret image extraction is done by the proposed technique in which first the cover image is recovered by noise removal methods and then applying alpha blending. Since peak signal-to-noise ratio (PSNR) is extensively used as a quality measure of stego images, the reliability of PSNR for stego images is also evaluated in the work described in this dissertation. The proposed work is compared with the existing method using PSNR, MSE, NCC, MAD, SC as comparison parameters. Proposed technique reduces the requirement to keep record of cover images for secret information extraction. Otherwise for each information received, the receiver should also have the cover image saved with him. In the proposed technique I have tried to obtain the secret image from stego image without having cover image, considering secret image as noise. The technique deals with steganography in wavelet domain. Complete work can be seen as adding noise to cover image, and then using noise removal technique to obtain secret image. Soft thresholding and bilateral filtering used for removing noise are efficient. Experimental results shows that there's a trade – off between stego image and secret image extracted. It is seen that as we increase the value of alpha, stego image degrades, but secret image improves. The secret image obtained is in visually acceptable form. Results shown are objective and subjective in nature.

Keywords- Alpha blending, Arnold transformation, Bilateral Filtering, DWT, Steganography, Soft Thresholding.

I. INTRODUCTION

Steganography means covered writing. Purpose of it is to hide the fact that communication is taking place. The word cover is used to describe the original, innocent message. Security is becoming more important as the amount of data being exchanged on the internet increases. Therefore to protect the data from unauthorized access confidentiality and integrity are required. This has resulted in the fast growth of information hiding techniques [1]. Sometimes it is not enough to keep the contents of message secret, it is also important to keep the existence of message secret. The technique used to implement this is known as steganography.

Revised Manuscript Received on 30 November 2013.
* Correspondence Author
Manisha Boora, Electronics and Communication, N. C. C. E., Israna, Panipat, India.
Monika Gambhir, Electronics and Communication, N. C. C. E., Israna, Panipat, India.

The word steganography is derived from Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images [2].

Cover Image: This is the original image into which required information is embedded. It is also termed as carrier image. The information should be embedded in such a manner that there are no significant changes in the statistical properties of cover image.

Stego Image: It is an image obtained by the combination of payload and cover image [3].

Due to inability to guarantee security , various vulnerabilities exist in the network that can be exploited and gives rise to several security attacks. To mitigate such security vulnerabilities and facilitate safe transfer of data over communication channel, techniques like cryptography, steganography are developed.Steganography is preferred over cryptography, because in cryptograohy the cipher text which is a scrambled text obtained from plain text and the attacker can guess that the encryption has been done and can apply decryption techniques to obtain the hidden data.On the contrary, steganography is the process of hiding data in some cover media like still images, audio, video . Therefore the attacker does not know that information is being transmitted, since it is hidden to the naked eye and impossible to distinguish from cover media.

A. Steganalysis

This is the practice of attacking stego image by detection, destruction, extraction, or modification of embedded data. By understanding the ways by which attackers can defeat steganographic models, it is necessary to design and develop more superior and robust methods. In steganography the meaning of successful attack means that the attacker is able to identify and has proof that some kind of data is hidden within the stego- image. Successful attack for a pirate attempting to defeat a copyright mark is that he detects and also destroys or modifies the watermark without significant degradation to the perceptual quality of stego- image. There are five categories in which steganalysis technique can be divided: stego only, known cover, known message, chosen stego, and chosen message. In stego - only attack, only the stego image is available for the attack. In know- cover attack , both original cover and stego image are available for steganalysis. The known - message attack is when steganalyst knows the secret message embedded in stego-image. A chosen- stego attack is when the attacker has the decoding algorithm. The chosen- message attack is when the steganalyst has access to encoding algorithm.

Presence of embedded data or watermark can be detected by analyzing the distortions that are present in the stego-image. The known- cover attack simplifies the analysis of distortions because the stego- image can be compared with the cover- image to determine the distortion. This is a challenging task to remove the embedded message without causing significant damage to the stego- image.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

This is because the embedding algorithms are designed with the assurance that the watermark can only be removed with significant damage to the stego- image [4].

II. RELATED WORK

S .K. Moon et al. [1] implemented 4LSB for color bitmap images (24 bit and 8 bit i.e. 256 color palette images) and wave files as the carrier media. By using this proposed algorithm, file of any format can be hidden in an image and audio file.

T. Morkel et al. [2] attempts to identify the requirements of a good steganographic algorithm and reflects on which steganographic techniques are more suitable for which applications.

K Suresh Babu* et al. [3] proposed Steganographic model Authentication of Secret Information in Image Steganography that can verify the reliability of the information being transmitted to the receiver. The method can verify whether the attacker has tried to edit, delete or forge the secret information in the stego-image. The method can verify whether each row has been modified or forged by the attacker.

Eugene T. Lin et al. [4] reviewed various techniques for data hiding in digital images. Features of steganographic systems were also discussed. Finally, an overview of steganalysis was presented.

S.Arivazhagan1 et al. [5] The work deals with Image steganalysis which focuses first in identifying the employed steganographic algorithm and this information is used in deciphering any hidden data in cover images. In this work the stego images are decomposed into its approximation and detail sub bands and from the decomposed sub bands, co-occurrence and statistical features are derived. This leads to detection of steganographic algorithm.

Zhenjun Tang et al. [10] designed an image encryption technique by combining Arnold transform and three random strategies . The security of the scheme depends on the random strategies.. The proposed encryption scheme is robust and secure. It has no size limitation, indicating the application to any size images.

III. PROPOSED METHOD

A. Discrete wavelet transform

Discrete Wavelet Transform provides a fast, local, sparse, multi-resolution analysis of real world signals and images.

It is useful for processing non-stationary signals. It decomposes signal into a set of basis functions, called wavelets. Wavelets are created by translations and dilations of a fixed function called mother wavelet.

Wavelet transform provides both frequency and spatial description of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. The main idea behind DWT results from multi-resolution analysis, which involves decomposition of an image in frequency channels of constant bandwidth on logarithmic scale. Image itself is considered as a two dimensional signal. DWT can be implemented as a multistage transformation. An image is decomposed into four sub- bands denoted as LL (Low-Low), LH (Low- High), HL (High- Low), HH (High-High) at level 1 in DWT domain. LL sub- band consists of low frequency wavelet coefficients

The LL sub- band can further be decomposed to obtain another level of decomposition. The decomposition process of the LL sub- band continues until the desired number of levels determined by the application is reached. When image is passed through a series of low pass and high pass filters, image is decomposed into sub- bands of different resolutions. At level 1 DWT decomposes image into four non- overlapping multiresolution sub- bands : LL_X (Approximate sub- band), LH_X (Vertical sub- band), HL_X (Horizontal sub- band), HH_X (Diagonal sub- band). Here LL_X is low frequency component, whereas LH_X , HL_X , HH_X are high frequency components. Maximum energy of images is concentrated in approximate sub-band and amplitude of coefficient is larger than the one of detail sub-graph. High frequency sub- bands of the wavelet transform include edges and textures, and other detailed information of the image and the human eye is not very sensitive to changes in such bands. Embedding is difficult to be detected in these parts, but it is easy to be destroyed and has poor stability after image processing.

To obtain next scale of wavelet coefficients after level 1, the sub- band LL_1 is further decomposed until final N scale is reached. When N is reached, there are 3N+1 sub- bands available where 'x' ranges from 1 to N. From these DWT coefficients, original image can be reconstructed. This reconstruction process is called inverse DWT (IDWT).

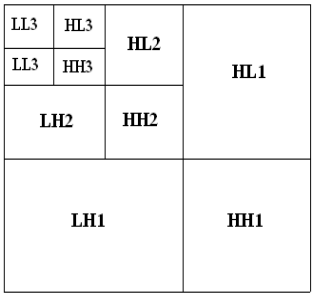

Fig. 1: Three Level Image Decomposition

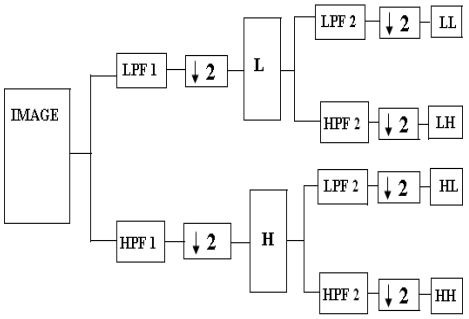

Fig. 2: One level decomposition using two dimensional DWT

LPF1 represents low pass filtering of image rows, HPF1 represents high pass filtering of image rows, LPF2 represents low pass filtering of image columns, HPF2 represents high pass filtering of image columns.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

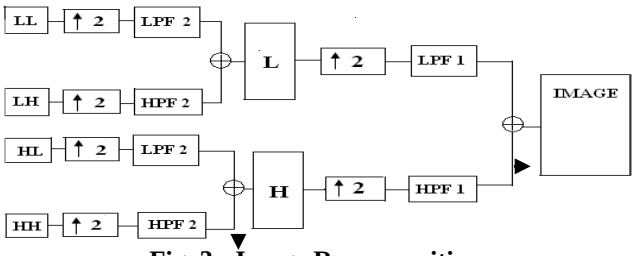

Fig. 3: Image Recomposition

Union of four sub- bands permits to reconstruct the original image. The LL subband comes from low pass filtering in both directions and is mostly like original image and so it is called as approximate component. The remaining sub-bands comes from the combination of low and high pass filter. Components obtained using only high pass filters are called as detailed components. LH preserves vertical edge details, HL preserves horizontal edge details and HH preserves the diagonal details [5][6][7].

B. Arnold transform

The image encryption algorithms can be classified into two kinds: One is; frequency-based method the other is spatial-based method. The spatial-based algorithms are generally achieved by altering pixel values or swapping the pixel positions. Arnold transform commonly known as cat face transform is an efficient technique for position swapping, and widely applied to image encryption. Encryption techniques also called image scrambling, produces an unintelligible or disordered image from the original image, therefore used to confirm the security and improve the robustness of the steganographic scheme. Therefore the secret image should be pre-processed before embedded into the original image. The transform rearranges the position of image pixels, and if it is done several times, a disordered image can be generated. The special property of Arnold Transform is that image comes to it's original state after certain number of iterations i.e. after iterating a certain numbers it returns the same pixels position as before and thereby produces the original image. . These' number of iterations' are called 'Arnold Period' or 'Periodicity of Arnold Transform'. The periodicity of Arnold Transform (P), is dependent on size of given image.

It is a one-to-one transformation applied on an image of dimensions N×N, represented by the equation

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N$$

(x , y) and (x' , y') $\in$ {0, 1, 2, ……..N-1}

where, A= $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$

The above equation rearranges each and every pixel coordinates of the images i.e. realigns the pixel matrix of digital image, where (x, y) is the location coordinates of the original image pixels and (x', y') is the location coordinates of image pixels that after transform. When all the coordinates are transformed, the image we obtain is scrambled image. *N* is the height or width of the square image processed.

N	2	3	4	5	6	7	8	9	10	11	12	16	24	25
Period	3	4	3	10	12	8	6	12	30	5	12	12	12	50
N	32	40	48	50	56	60	64	100	120	125	128	256	480	512
Period	24	30	12	150	24	60	48	150	60	250	96	192	120	384

Fig 4. Relation between size of image and period

Figures below represent the Arnold transform process with 8×8 image. In Figure 5, Figure 5a is the original image, with its matrix message in Figure 5b, and Figure 5c-5h show the matrix message from one to six-time Arnold transform.

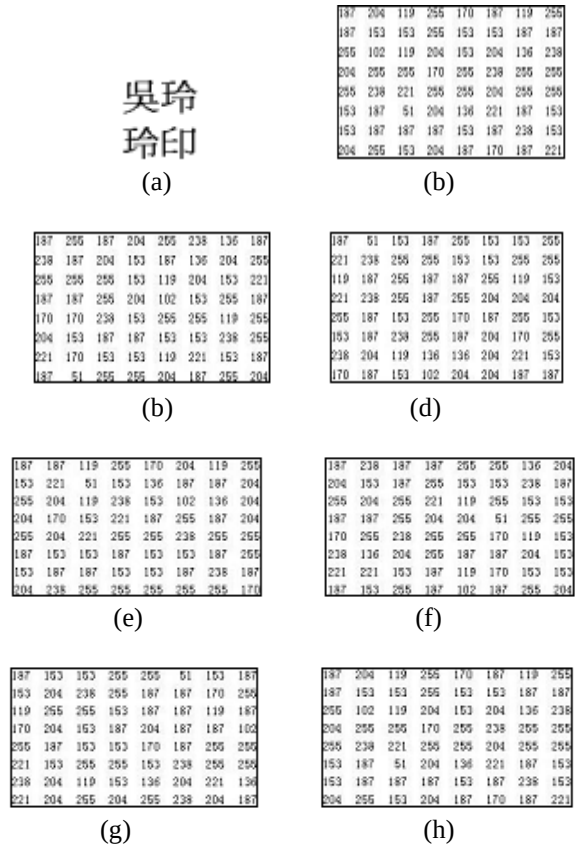

Fig. 5: Arnold transform process with 8×8 image

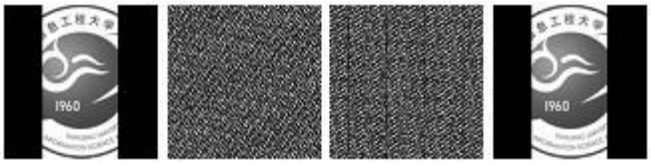

Fig. 6: Image before 20(60, 96) time Arnold transform with cut original image

Figure 6a is the 128×128 original image. Fig. 6(b)-(d) shows the image thorough 20/60/96 times Arnold transform. Arnold transform based schemes have a common weakness that image height must equal image width.

If one image iterates *m* steps to get scrambled state with Arnold transformation, it can restore its image with the same steps form the scrambled state by anti-Arnold transformation [8-13].

C. Alpha Blending

It is the way of mixing two images together to form a stego image. In this technique the decomposed components of the host image and the secret image are multiplied by a scaling factor and are added.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

It can be accomplished by blending each pixel from the secret image with the corresponding pixel in the cover image. The equation for executing alpha blending is as follows,

Stego Image = k*(LL3) +q*(Secret Image) where, k and q are scaling factors

The blending factor used in the blended image is called the "alpha."

Formula of the alpha blending extraction to Recover secret image is given by

Secret Image = (Stego Image – Cover Image) /q [14-15].

D. Implementation

The following session describes the implementation of the encoding and decoding process clearly. The encoding process includes DWT, Arnold transformation, Alpha blending, IDWT and Stego image formation. The decoding process includes DWT, Arnold transformation, Alpha blending, IDWT and Secret image formation.

1. Encoding Process

During encoding process the cover image and scrambled secret image(i.e. with key) are DWT transformed and then alpha blended**.** Next, IDWT was performed to reform the stego image.This secure stego image was transferrred to any communication media. The secret key and alpha blending operation gives more security.

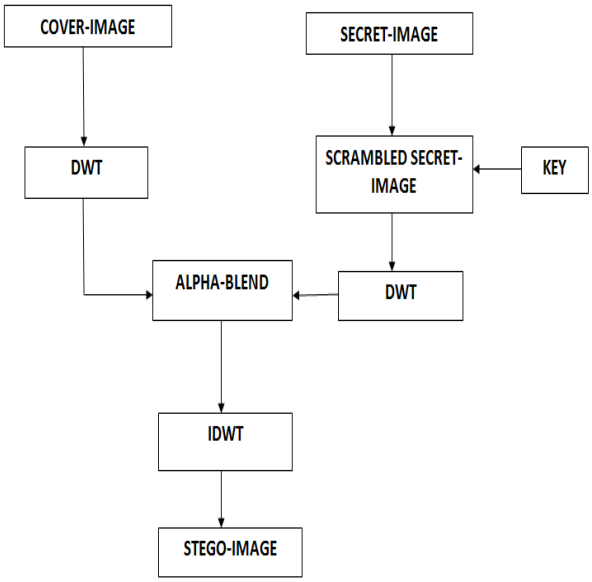

Fig. 7: Encoding process(Existing Work)

1. Preprocessing both the cover image(N*N) and secret image(N*N).
2. Perform 2-D discrete wavelet transform(DWT) of cover image(N*N).
3. Apply private key with Arnold transformation on secret image and get the scrambled secret image(scrambling provides security and applying key further increases the security level).
4. Perform 2-D DWT of the secret image image(N*N).
5. Extract the approximation co-efficient of matrix(LL) and detail coefficient matrices LH, HL& HH of cover image.
6. Next extract the approximation co-efficient of matrix LL and detail coefficient matrices LH, HLand HH of the scrambled image.
7. Apply alpha blending on cover image and secret image.
8. Perform 2-D IDWT (Inverse discrete wavelet transform) to form stego image.

1. Decoding Process

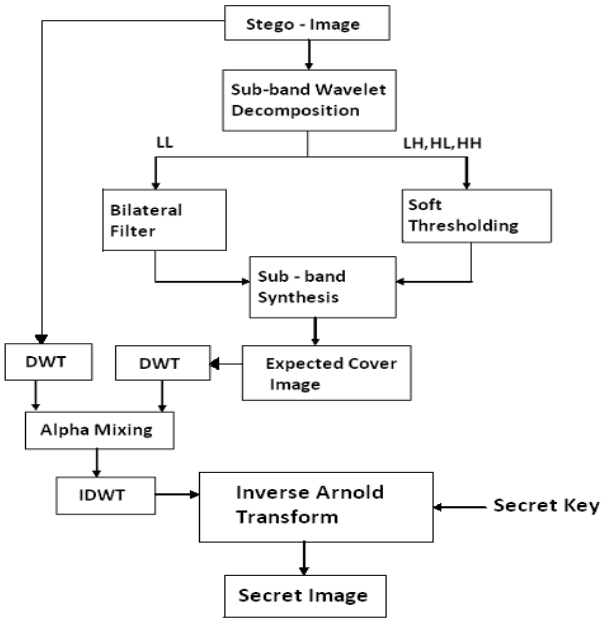

Fig. 8: Decoding process (Proposed Work)

1. Receive the stego image.
2. Perform 2-D DWT on the stego image and obtain frequency components LL, LH, HL, HH.
3. Pass approximate coefficient LL through bilateral filter and perform soft thresholding on other detailed coefficients.
4. Synthesize the outputs after performing bilateral filtering and soft thresholding and obtain required cover image.
5. Perform DWT on recovered cover image and stego image.
6. Apply alpha blending on wavelet transformed stego image and cover image.
7. Take IDWT to obtain scrambled image.
8. Perform Arnold Transformation with key and get the original secret image.

IV. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

Implementation of the proposed method has been done using Matlab R2007a.

Experimental Design: Mainly, five grayscale images: Lena, Barbara, Goldhill, Peppers,each of 256x256 pixels were arbitrarily selected, Barbara is originally taken of size 512x512 pixels and used as cover images. All the images are resized to 512x512. However, the only reason for choosing these images is being well-known and commonly used in the areas of digital image processing, compression and steganography. Additionally, the variables used to evaluate the performance of proposed method are PSNR, NCC, MSE, MD, SC. The experimental results are for only binary text images (secret images). Bayes Shrink is used for soft thresholding.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

TABLE-I COMPARISON OF VARIOUS QUALITY MEASUREMENTS

COVER IMAGE	SECRET IMAGE	PSNR	MSE	NCC	MD	S C	ALPHA
1) Lenna.tiff 256×256	Image1.bmp 403×327	24.5116	5.5228e+007	0.9093	5.6843e-014	0.8285	0.06
2) Barbara.png 512×512	Name.bmp 403×327	24.8025	5.2500e+007	0.9129	5.6843e-014	0.8357	0.06
3) Goldhill.tiff 256×256	Image2.bmp 403×327	24.7838	5.2727e+007	0.9069	5.6843e-014	0.8248	0.06
4) Peppers.tiff 256×256	Image3.jpeg 400×325	24.5510	5.1200e+007	0.9158	5.6843e-014	0.8409	0.06
5) Lenna.tiff 256×256	Image1.bmp 403×327	30.5322	1.3807e+007	0.9530	2.8422e-014	0.9087	0.03
6) Barbara.png 512×512	Name.bmp 403×327	30.8231	1.3125e+007	0.9551	7.1054e-014	0.9130	0.03
7) Goldhill.tiff 256×256	Image2.bmp 403×327	30.8044	1.3182e+007	0.9518	2.8422e-014	0.9067	0.03
8) Peppers.tiff 256×256	Image3.jpeg 400×325	30.5716	1.2800e+007	0.9567	5.6843e-014	0.9159	0.03

SUBJECTIVE RESULTS:

Extracted Secret Image(Proposed Technique)

Extracted Secret Image(Existing Technique)

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

V. CONCLUSION AND FUTURE WORK

In the proposed technique it is tried to obtain the secret image from stego image without having cover image, considering secret image as noise. Complete work can be seen as adding noise to cover image, and then using noise removal technique to obtain secret image. This work deals with secret images as binary text images, with text particulary to be black. Experimental results shows that there's a trade – off between stego image and secret image extracted. It is seen that as we increase the value of alpha, stego image degrades but the secret image becomes more visually acceptable. The information retrieved is of visually acceptable form. Proposed technique reduces the requirement to keep record of cover images for secret information extraction. Otherwise for each information received, the receiver should also have the cover images saved with him, which he should recall everytime for each information extraction. Although the results obtained with previous technique were better, but the proposed technique also fulfills the requirement of a steganographic system, with a large advantage over it. In addition, there is a trade-off between both steganographic capacity and stego image quality. Hiding more data in cover images (higher capacity) introduces more artefacts into cover images and then increases the perceptibility of hidden data . Furthermore, it is not possible to simultaneously maximize the security and capacity of a steganographic system. Therefore, increasing steganographic capacity and enhancing stego image quality are still challenges. Future Work: Experiments can be done for secret images not particulary be text. The work can be extended for color images. One can further try to improve the extracted secret image quality.

REFERENCES

1. S .K. Moon and R.S. Kawitkar, "Data Security using Data Hiding", International Conference on Computational Intelligence and Multimedia Applications, vol.- 04, pp. 247-251, Dec. 2007.
2. T. Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science, 2005
3. K Suresh Babu* et. al., "Authentication of Secret Information in Image Steganography", pp. 1-6, Nov. 2008, IEEE .
4. Eugene T. Lin and Edward J. Delp," A Review of Data Hiding in Digital Images".
5. S.Arivazhagan,W.Sylvia Lilly Jebarani,, M.Shanmugaraj,"An Efficient Method for the Detection of Employed Steganographic Algorithm using Discrete Wavelet Transform", Second International conference on Computing, Communication and Networking Technologies, pp.1-6, 2010.
6. Chih-Chin Lai,Member, and Cheng-Chih Tsai," Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", Ieee Transactions on Instrumentation and Measurement, Vol. -59, No. -11, pp. 3060- 3063, November 2010.
7. B.L. Gunjal, R.R.Manthalkar," Discrete Wavelet Transform based Strongly Robust Watermarking Scheme for Information Hiding in Digital Images", Third International Conference on Emerging Trends in Engineering and Technology, pp. 124- 129, 2010 IEEE.
8. Ma Ding, Fan Jing," Digital Image Encryption Algorithm Ba sed on Improved Arnold Transform", International Forum on Information Technology and Applications, Vol. -1, pp. 174- 176, 2010.
9. Sudhir Keshari, Dr. S. G. Modani," Image Encryption Algorithm based on Chaotic Map Lattice and Arnold cat map for Secure Transmission", International Journal of Computer Science and Technology(IJCST), Vol.- 2, Issue - 1, March 2011
10. Zhenjun Tang and Xianquan Zhang," Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies", Journal of Multimedia, Vol.- 6, No.- 2, pp. 202- 206, April 2011.
11. Divya saxena," Digital Watermarking Algorithm based on Singular Value Decomposition and Arnold Transform", International Journal of Electronics and Computer Science Engineering, pp. 22- 27.
12. Lingling Wu, Jianwei Zhang, Weitao Deng, Dongyan He," Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm", The 1st International Conference on Information Science and Engineering (ICISE2009), pp. 1164- 1167, IEEE 2009
13. B.L. Gunjal, R.R.Manthalkar," Discrete Wavelet Transform based Strongly Robust Watermarking Scheme for Information Hiding in Digital Images", Third International Conference on Emerging Trends in Engineering and Technology, pp. 124- 129, IEEE 2010.
14. Kalra, G.S., R. Talwar and H. Sadawarti," Blind Digital Image Watermarking Robust Against Histogram Equalization", Journal of Computer Science 8 (8), pp. 1272- 1280, 2012.
15. Baisa L. Gunjal, and Suresh N.Mali," Secured Color Image Watermarking Technique in DWT- DCT Domain", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.1, No.3, pp. 36- 44, August 2011.
16. Nilanjan Dey, Sourav Samanta, Anamitra Bardhan Roy," A Novel Approach of Image Encoding and Hiding using Spiral Scanning and Wavelet Based Alpha-Blending Technique", Int. J. Comp. Tech. Appl., Vol. 2 (6), pp. 1970-1974, 2011.

AUTHOR PROFILE

A Manisha Boora received the B.Tech degree in Electronics and Communcation from Lingaya's Institute of Management and Technology, Faridabad, affiliated to Maharshi Dyanand University, Rohtak, India in 2011. She is persuing M.Tech in Electronics and Communication, from N.C. College of Engineering,Panipat, India. Her area of interest is Image Processing.

Monika Gambhir received the M.Tech degree in Electronics and Communcation from N.C. College of Engineering, Panipat, India.She is working as Assistant Professor there. Her area of interest is Digital Image Processing.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)