Arnold Transform Based Steganography

Manisha Boora, Monika Gambhir

***Abstract** — Steganography exploits the use of host data to hide a piece of information in such a way that it is imperceptible to human observer. Its main objectives are robustness, high payload, and imperceptibility. Digital images, videos, sound files, and other computer files can be used as carrier to embed the information. This paper deals with digital gray scale digital images, and presents a secure steganography scheme for hiding a larger size secret-image into smaller size cover- image. Arnold Transformation is performed to obtain scrambled secret image. Discrete Wavelet Transform (DWT) is performed on both host / cover image and secret image / information, and this is followed by alpha blending operation. The approach shows satisfactory results. Results show that proposed algorithm is highly secured with good perceptual invisibility.*

***Keywords**— Alpha Blending, Arnold Transformation, DWT, Steganography.*

I. INTRODUCTION

The word steganography is derived from Greek words “stegos” meaning cover and “grafia” meaning writing.In image steganography information is hidden in images.

Since the rise of Internet one of the most of the important factors of information technology and communication has been the security of information. Sometimes it is not enough to keep the contents of the message secret, it is also necessary to keep the existence of the message secret. Steganography is one such technique to implement this. Steganography is the art and science of invisible communication. This is accomplished through hiding information in another information, thus hiding the existence of communicated information[1]. The reason for this security and confidentiality is because the communication network over which the transfer of information takes place is unreliable and unsecured. Anybody with proper knowledge and right applications can eavesdrop and learn of the communication and intercept the data transfer which could be very dangerous and even life threatening in some situations.

In ideal condition, internet, routing protocols and communication network should exhibit these properties :

Reliability**:** Internet should ensure the reliable delivery of information to the intended receiver.

Fault Tolerance**:** This means the ability of the system to operate normally even in situations of failure. Therefore, internet should exhibit fault- tolerance so as to keep on functioning even under conditions of failure in some part of internet.

Security**:** The security provided by internet should be such that only the intended recipient should have access to the information.

All the above properties are ideal and cannot be implemented practically completely in the functioning of internet. One of the property that cannot be guaranteed in the in the internet is security[2][3][4][5][6].

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 cryptography 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.

II. RELATED WORK

Po-Yueh Chen* et al. [7] have proposed secrete message is embedded into the high frequency co-efficient of the wavelet transform while leaving the low frequency co-efficient sub-band unaltered.

S.Arivazhagan1 et al. [8] describes a generic steganalytic scheme that builds a feature database from statistical and Co-occurrence features extracted from DWT decomposition. Though the classifier needs to be checked with a very large database, results are promising to provide useful information to the Steganalyst.

R. Talwar et al. [9] proposed a robust blind watermarking algorithm based on Arnold-Chaoss encryption and combined discrete wavelet transform-discrete cosine transformation. Dual encryption technique is deployed to enhance the security of the watermark. The watermark become more secure because the pseudo-random sequence generated by Arnold and chaos system possesses feature of very high randomness.

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

Pratibha Sharma et al. [13] presented a 3 level DWT based image watermarking technique. This technique can embed the invisible watermark into the image using alpha blending technique which can be recovered by extraction technique. In this technique a multi-bit watermark is embedded into the low frequency sub-band of a cover image by using alpha blending technique. During embedding, watermark image is dispersed within the original image depending upon the scaling factor of alpha blending technique. Extraction of the watermark image is done by using same scaling factor as for embedding.

Manuscript received September, 2013.

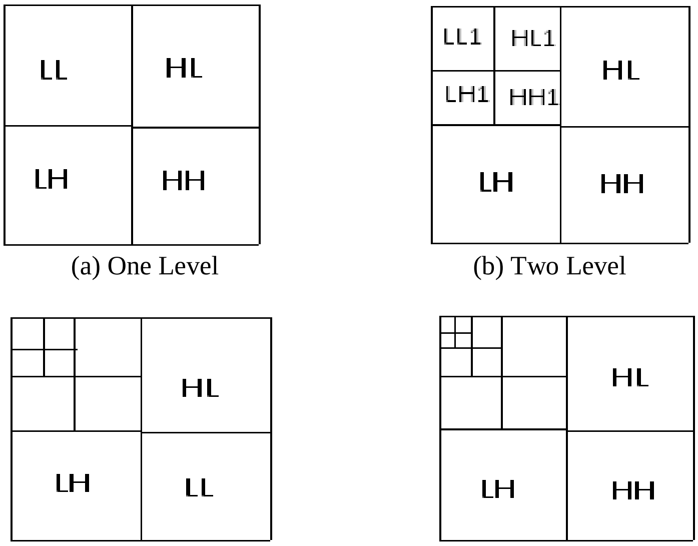
Manisha Boora, Electronics and Communication, N.C.C.E., Israna,Panipat, India.

Monika Gambhir, Electronics and Communication, N.C.C.E., Israna, Panipat, India.

III. PROPOSED METHOD

A. Dwt

Discrete Wavelet Transform provides a multiresolution analysis of real world images and signals.



(a) One Level (b) Two Level

(c) Three level (d) Four level

Fig. 1: Decomposition of an Image using DWT

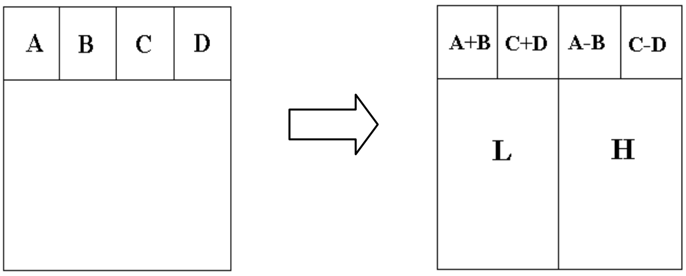


Fig. 2: The horizontal operation on the first row

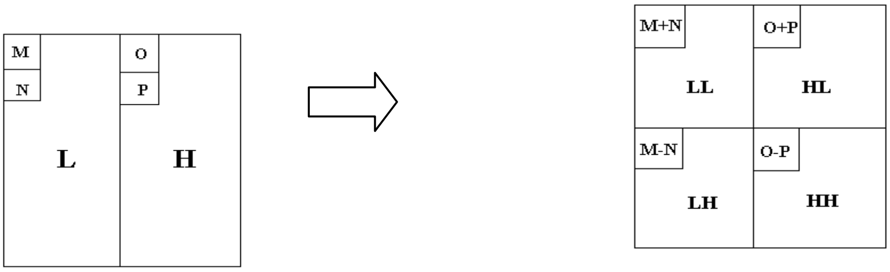
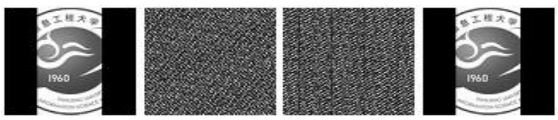


Fig. 3: The vertical operation

A 2-dimensional Haar-DWT comprises of two operations:one is horizontal operation and other is vertical operation. Step 1: first scan the pixels from left to right in horizontal direction and then perform the addition and subtraction operations on neighbouring pixels. Store sum on left and difference on right. Repeat this until all the rows are processed. Sum represents the low frequency part (L) and difference represents high frequency part (H) of the original image.

Step 2: Scan the pixels from top to bottom in vertical direction. Perform addition and subtraction on neighbouring pixels, and store the sum on top and difference on bottom. Repeat this until all the columns are processed. Finally 4 sub- bands are obtained known as LL, LH, HL, HH. LL sub-band is low frequency band and is much similar to original image. This is also known as the approximation sub- band, as it is an approximation of original image. LL sub- band can be decomposed further to obtain higher level DWT. LH, HL, HH are the detailed vertical , horizontal, diagonal sub-bands, respectively.[7][8]

B. Arnold Transform



(a) (b) (c) (d)

Fig. 4: 128×128 Image with 20(60, 96) time Arnold transform

Arnold Transform is commonly known as cat face transform and is only suitable for N×N images digital images. It is defined as $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$mod N (x , y) and (x' , y') {0, 1, 2, ………………..N-1} where (x, y) are the coordinates of original image, and (x',y') are the coordinates of image pixels of the transformed image. Arnold Transform is commonly known as cat face transform and is mainly suitable for digital images of size N×N. It is defined as $\begin{pmatrix} x\prime \\ y\prime \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$mod N, (x,y) and (x' , y') ε{0, 1, 2, ………………..N-1}, where (x,y) are the coordinates of original image and (x' , y') are the coordinates of image pixels of the transformed image. Transform changes the position of pixels and if done several times, scrambled image is obtained. N is the height or width of the square image to be processed. Arnold Transform is periodic in nature. The decryption of image depends on transformation periods. Period changes in accordance with size of image. Iteration number is used as the encryption key. When Arnold Transformation is applied, the image can do iteration, iteration number is used as a secret key for extracting the secret image[9]-[11].

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. 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 [12][13]

Alpha blending is the technique of mixing the cover image with the secret image. Value of alpha determines the level of mixing.

D. Implementation of steganography model

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 transferred to any communication media. The secret key and alpha blending operation gives more security. Preprocessing both the cover image(N*N) and secret image(N*N).

1. Perform 2-D discrete wavelet transform(dwt) at level 2 of cover image(N/4*N/4).
2. 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).
3. Perform 2-D dwt at level 2 of the secret image image(N/4*N/4).
4. Extract the approximation co-efficient of matrix(LA) and detail coefficient matrices LH, LV& LD of level 2 of cover image.
5. Next extract the approximation co-efficient of matrix LA1 and detail coefficient matrices LH1, LV1 and LD1 of level 2 of the scrambled image.
6. Apply alpha blending on cover image and secret image.
7. Perform 2-D IDWT (inverse discrete wavelet transform) to form stego image.

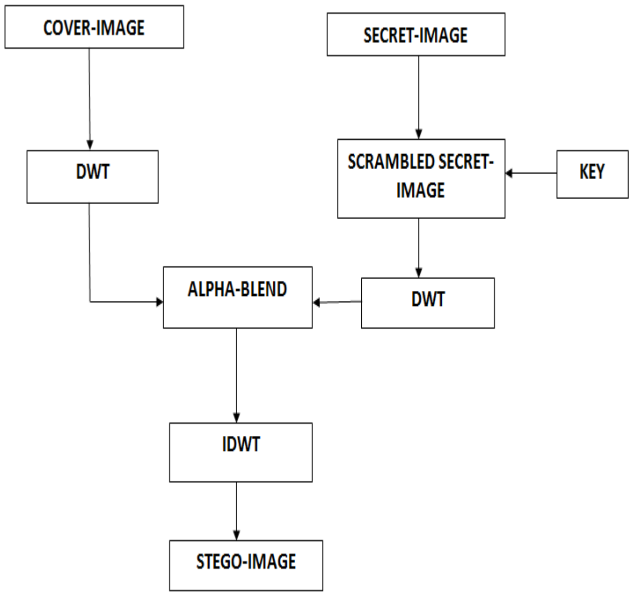


Fig 3.1: Encoding process

2) Decoding Process:

The recovered stego image and known cover image is reconstructed with DWT tarnsform and followed by alpha blending process.Next, IDWT is performed to rebuild the scrembled secret image. Finally the secret key is applied to get the original image.

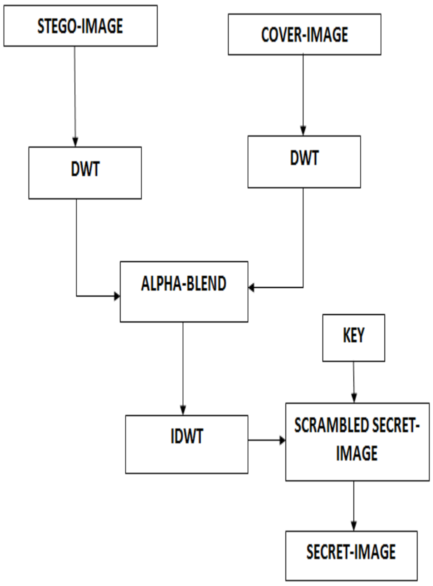


Fig 3.2: Decoding process

1. Receive the stego image.
2. Perform 2-D DWT at level 2 of the stego image amd cover image.
3. Apply alpha blending on both stego image and cover image.
4. Separate wavelet coefficients and take IDWT to reform scrambled image.

IV. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

Results shown here are the outcomes of embedding done in complete image i.e. in all sub-bands. Peak Signal To Noise Ratio(PSNR), Normalized Cross Corelation(NCC), Mean Square Error(MSE), and Mean Absolute Difference(MAD) are the parameters used for evaluating the performance of the proposed technique. Peak Signal to Noise Ratio Measures the distortion between original cover image and stego image.Higher the value of PSNR low is the distortion and vice- versa. MSE corresponds to the diference between the cover image and stego image. For high efficiency of Steganographic algorithm there should be minimum difference between stego image and cover image. Higher MSE value signifies more difference.

NCC measures the degree of similarity between cover image and stego image. Its value should be high. Maximum value of NCC is 1.

It is observed that as the value of alpha increases from 0.01 efficiency of the algorithm degrades. But as we decrease its value results are more acceptable as value of PSNR increases, NCC increases, and MSE decreases.

TABLE-I
COMPARISON OF VARIOUS QUALITY MEASUREMENTS ON COVER IMAGES AND STEGO IMAGE WITH SECRET IMAGES

COVER IMAGE	SECRET IMAGE	PSNR	MSE	NCC	ALPHA
1) Boat.png 512×512	Barbara.png 512×512	45.8873	4.3943e +005	0.9920	0.01
2) Barbara.png 512×512	Lenna.tiff 256×256	45.3571	4.6207e +005	0.9914	0.01
3) Peppers.tiff 256×256	Baby.jpg 600×420	44.2482	1.4193e +005	0.9923	0.01
4) Boat.png 512×512	Barbara.png 512×512	45.0594	5.3171e +005	0.9912	0.011
5) Barbara.png 512×512	Lenna.tiff 256×256	44.5292	5.5910e +005	0.9905	0.011
6) Peppers.tiff 256×256	Baby.jpg 600×420	43.1633	1.7174e +005	0.9918	0.011
7) Boat.png 512×512	Barbara.png 512×512	46.8024	3.5594e +005	0.9928	0.009
7) Barbara.png 512×512	Lenna.tiff 256×256	46.2722	3.7427e +005	0.9922	0.009
8) Peppers.tiff 256×256	Baby.jpg 600×420	44.9063	1.1496e +005	0.9933	0.009
9) Boat.png 512×512	Barbara.png 512×512	47.8255	2.8124e +005	0.9936	0.008
10) Barbara.png 512×512	Lenna.tiff 256×256	47.2953	2.9572e +005	0.9931	0.008
11) Peppers.tiff 256×256	Baby.jpg 600×420	45.9293	9.0836e +004	0.9940	0.008
12) Lenna.tiff 256×256	Goldhill.tiff 256×256	51.8640	2.4575e +004	0.9961	0.005
13) Barbara.png 512×512	Lenna.tiff 256×256	51.3777	1.1552e +005	0.9957	0.005
14) Peppers.tiff 256×256	Baby.jpg 600×420	50.0117	3.5483e +004	0.9963	0.005

V. CONCLUSION

This work deals with the techniques for steganography in discrete wavelet transform as associated to gray scale images and binary images. A new and secure steganography method for embedding secret image into cover image without producing any major change has been proposed. In future secret image could be extracted only with stego image without the availability of cover image.

REFERENCES

[1] Po-Yueh Chen*and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, pp. 275-290, vol.- 4,Issue- 3, 2006

[2] Bhavyesh Divecha, Ajith Abraham, Crina Grosan and Sugata Sanyal, "Analysis of Dynamic Source Routing and Destination-Sequenced Distance-Vector Protocols for Different Mobility models", First Asia International Conference on Modeling and Simulation, AMS2007, 27-30 March, 2007, Phuket, Thailand. Publisher: IEEE Press, pp. 224-229.

[3] S. Gowrishankar, S. Sarkar, T.G.Basavaraju, "Simulation Based Performance Comparison of Community Model, GFMM, RPGM, Manhattan Model and RWP-SS Mobility Models in MANET," First International Conference on Networks and Communications (NETCOM '09), 27-29 Dec. 2009, pp.408-413.

[4] Jonghyun Kim, Vinay Sridhara, Stephan Bohacek, "Realistic mobility simulation of urban mesh networks", Journal of Ad Hoc Networks, Vol. 7, Issue 2, March 2009, Publisher: Elsevier, pp. 411-430.

[5] Liu Tie-yuan, Chang Liang, Gu Tian-long, "Analyzing the Impact of Entity Mobility Models on the Performance of Routing Protocols in the MANET", 3rd International Conference on Genetic and Evolutionary Computing, 14-17 Oct. 2009, pp.56-59.

[6] M.F. Sjaugi, M. Othman, M.F.A. Rasid, "Mobility models towards the performance of geographical-based route maintenance strategy in DSR", IEEE International Symposium on Information Technology, ITsim 2008 , Vol. 3, 26-28 Aug. 2008, pp. 1-5.

[7] Po-Yueh Chen*and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, pp. 275-290, vol.- 4,Issue- 3, 2006

[8] S.Arivazhagan, W.Sylvia Lilly Jebarani, M.Shanmugaraj," An Efficient Method for the Detection of Employed Steganographic Algorithm using Discrete Wavelet Transform", pp. 1-6, Second International conference on Computing, Communication and Networking Technologies,2010 IEEE.

[9] Kalra, G.S., R. Talwar and H. Sadawarti," Blind Digital Image Watermarking Robust Against Histogram Equalization", Journal of Computer Science 8 (8): 1272-1280, 2012.

[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, April 2011

[11] 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

[12] 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

[13] Pratibha Sharma, Shanti Swami," Digital Image Watermarking Using 3 level Discrete Wavelet Transform", Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013), pp. 129- 133, 2013

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.