Information Secrecy in digital Images Based on Noise Removal Algorithms and Arnold Transformation Using Watermark

S.Venkatesh[1] , Dr.M.A.Dorairangaswamy[2]
[1] Research Scholar, Faculty of Computer Science and Engineering
Sathyabama University, Chennai, Tamilnadu.
[2]Professor and Registrar, St Peter's University, Avadi Chennai, Tamilnadu.
[1]venkyjep@gmail.com
[2] drdorairs@yahoo.co.in

Abstract - **Secret writing techniques have been used for centuries. Using Secret Writing of secret message can be embedded inside a piece of unsuspicious information and transfer it without anyone's information about the existence of the secret message. This paper introduces Color image Secret writing utilizing image noise removal algorithm by wavelet thresholding. Wavelet transform is employed to represent spatial area image into time occurrence domain. At first the preprocessed color cover image is transmitted from RGB to YIQ Tint model in arrange to take out its I-component. At the same time, Arnold Transformation is performed to mix up the secret message then together cover-I and secret message are decomposed using Discrete Wavelet Transform (DWT). In general secret data is hidden in noisy components of cover medium, this implies that calculate a entry base on wavelet coefficients of wrap image to determine the noisy components. Afterwards the normalized secret message Alpha combination with the cover-I. This proposed method improves the capacity, Peak Signal to Noise Ratio (PSNR), provide elevated security and certain robustness.**

Keywords - Noise Removal Methods, Arnold Transformation, Image quality Metrics, DWT.

I. INTRODUCTION.

With the current advance in multimedia relations and its power in our electronic world, the significance of in sequence security has been severely increased. Existing technologies in the field of information security system offer conceal the happening of message for anyone except the intended recipient. In this way, Secret characters provide a dependable answer for embed a secrete data into a cover media imperceptibly. Basically, the ultimate objectives of Secret writing are undetectability, strength, and elevated capacity of the concealed data that separate it from interrelated technique such as watermarking. Also, the hidden message can be recovered using appropriate key without any information of the unique cover media. In general, Secret writing algorithms usually struggle with achieve a elevated embedding charge, large ability, and high-quality imperceptibility. This job aims to near an efficient s Secret writing technique in image files. The most common Secret writing techniques in digital images focus on spatial domain methods-which generally use a direct smallest amount Significant Bit alternate technique- and frequency domain methods such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and soon.

II. Methodology.

A. Pre-processing

Histograms are function describe the in sequence extracted from the image. The histogram function is definite over all probable intensity level.

B. Separate Transform

This convert is based on filtering the image coefficients on a raw-by-raw and vertical-by-vertical basis repetitively. Double-dimensional wavelets decay is same as basic one which leads to a decomposition of estimate coefficients at level *j* in four mechanisms: the approximation at level *j+1,* and the particulars in three details in three orientations; flat, perpendicular and slanting as shown in Fig. 1. The low-pass and high pass filters of the wavelet transform logically break a indication into similar and discontinuous or rapidly-changing sub signals, respectively. The slow altering aspects of a indication are potted in approximation which include low-pass group. On the other hand, a feature band consists of elevated frequency coefficients, which contain rim details of spatial domain picture, sound components, and the quickly altering parts. Therefore we can implant data in the region that human vision is fewer responsive to, such as the high declaration detail band where generally contains noisy components., the basic idea of noise removal is to decrease high frequencies, because sound is always presented by elevated frequencies. As a result, most noise removal techniques tend to suppress elevated frequencies. These noisy wavelet coefficients have the potency to hide secret information.

C Arnold transform

Arnold Transform is commonly known as cat face transforms and is only suitable for N×N images digital images. It is defined as

$$\begin{pmatrix} x\prime \\ y\prime \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (mod\ N) \quad (1)$$

Where (x, y) are the coordinates of original image, and (x',y') are the coordinates of picture pixels of the distorted image. Transform changes the position of pixels and if done numerous times, twisted image is obtained. N is the height or width of the rectangle image to be process. Arnold Transform is periodic in natural world. The decryption of image depends on alteration periods. Period changes in agreement with dimension of image. Iteration numeral is used as encrypting key. When Arnold Transformation is applied, the image can do iteration, iteration numeral is use as a secret solution for extracting the secret image.

D. Generic Blind Image Secret writing *System*

A message is embedded in a digital image by the embedding function, which uses a key or password. The resultant stego-picture is transmitting over a guide to the recipient, where it is processed by the extracting purpose using the similar key. During broadcast, the stego image can be monitored by unintended viewers who will notice only the allowance of the inoffensive image without discover the existence of the hidden message.

The parameter of Secret writing system, such as the numeral of data bits that can be hidden, the invisibility of the point, and its confrontation to removal, can be related to the individuality of communication systems such as ability and Peak Signal-to-Noise Ratio (PSNR). The notion of capacity in data hiding indicates the greatest number of bits hidden and productively improved by the stegosystems.

E. Threshold Selection Based on noise removal Methods

The collection of threshold calculation method is the main issue of wavelet threshold noise removal in the proposed method. Generally calculation of the threshold is done via statistical means in image noise removal. It can be solved using two basic approaches, spatial filtering methods and transform domain filtering methods. Spatial Filtering is a simple way to remove noise from image data which uses a fixed or adaptive threshold to recover the corruption of noise in digital image acquisition and transmission phase. As a vast literature has emerged recently on image noise removal via wavelet thresholding or shrinkage that is firstly introduced by Donoho and Johnstone. Based on Donoho report, σ is estimated using detail coefficient of wavelet transform as in equation (2)

$$\sigma = 1/0.6545(\ median(\ |c|\ ))\quad (2)$$

Where c is the detail coefficients of wavelet transform. Imagine n_c as the number of all the wavelet coefficients and c_{fs} as content all the wavelet coefficients.

Donoho universal method threshold as follow as in equation (3)

$$T\ Donoho\ = \sigma \sqrt{}(2\ log(N))\quad (3)$$

Where N is the size of considered wavelet coefficients.

The mini max principle is used in statistics in order to design estimators. Since the denoised signal can be assimilated to the estimator of the unknown regression function, the mini max estimator is the one that realizes the minimum of the maximum mean square error given in equation (4)

$$T\ mini\ max = 0.3936 + 0.1829(\ log(N)/log(2))\quad (4)$$

The above described threshold calculation methods are considered in the study as a modification to improve parameters of Secret writing system.

F. The Proposed Embedding Method

The fundamental concept of proposed method is the embedding of the hidden information with noise data of an color cover image, which is originally, spreads over cover image. Generally, an approximation coefficient of wavelet transform have no noisy pattern and are not suitable for embedding because they carry the most information content of the whole cover image. Therefore, details coefficient are the most convenient noisy area for embedding a secret data. Block diagram of the proposed defined over all possible intensity levels. For each intensity level, its value is equal to the number of the pixels with that intensity. Adaptive histogram equalization uses the histogram equalization mapping function supported over a certain size of a local window to determine each enhanced density value. Therefore regions occupying different gray scale ranges can be enhanced simultaneously. stego image can be monitored by unintended viewers who will notice only the transmittal of the innocuous image without discovering the existence of the hidden message. The parameters of Secret writing system, such as the number of data bits that can be hidden, the invisibility of the message, and its resistance to removal, can be related to the characteristics of communication systems such as capacity and Peak Signal-to-Noise Ratio (PSNR). The notion of capacity in data hiding indicates the maximum number of bits hidden and

successfully recovered by the secret writing system is depicted in Figure (1) and Figure (2) below. According to this figure, the process of the embedding and extracting the secret data can be described as follow:

Algorithm for *Embedding* Process:

Step-1: Preprocessing the cover Image and Secret Message

Step-2: Convert cover Image from RGB to YIQ color model and extract the I component.

Step-3: Arnold Transformation with key takes place to scramble the secret message.

Step-4: 2-D DWT Transformation takes place on both I component of cover image and secret message.

Step-5: Threshold will be calculated using noise removal method using 2-D DWT coefficients of cover Image.

Step-6: Normalize the DWT coefficients of message to threshold

Step-7: Threshold DWT coefficients of cover image are Alpha blending with normalized DWT coefficients of message.

Step-8: Inverse DWT can takes place to form the Stego image .

Step-9: Merge the Stego image into I component original YIQ cover image.

Step-10: Again convert the cover image from YIQ to RGB to get final Stego Image

Algorithm for Extracting Process:

Step-1: Convert the Stego image from RGB to YIQ and extract the I component.

Step-2: 2-D DWT Transformation has been takes place on I component.

Step-2: Threshold will be calculated using denoising method using 2-D DWT coefficients of Stego Image

Step-3: Normalize the DWT coefficients of message to threshold

Step-4: Inverse Alpha blending process

Step-5: Inverse DWT Transformation

Step-6: Arnold Transformation with same key on Embedding takes place to reconstruct the original Image.

Step-7: Secrete Image formation.

Embedding Process:

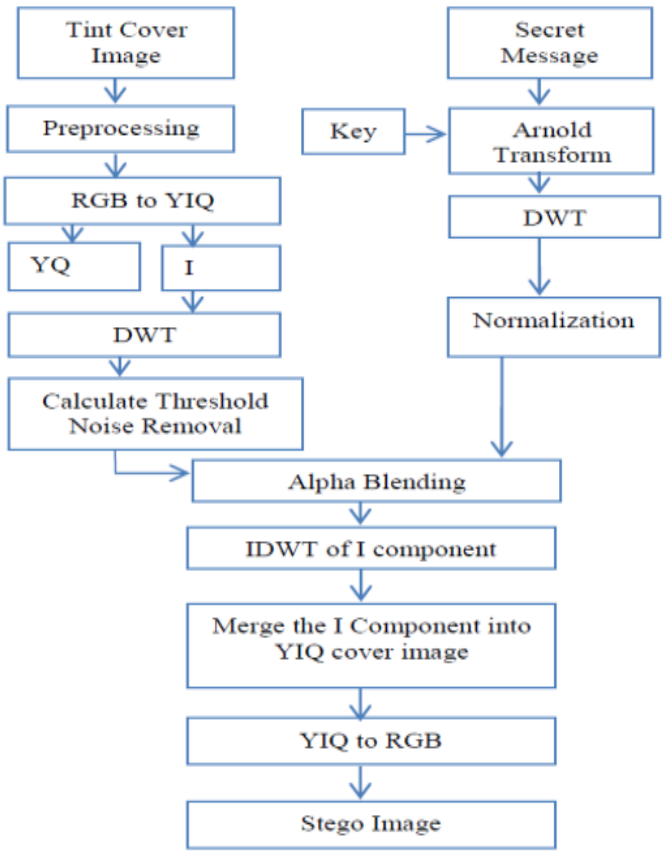

Fig.1 Block diagram of Proposed method (Encoding)

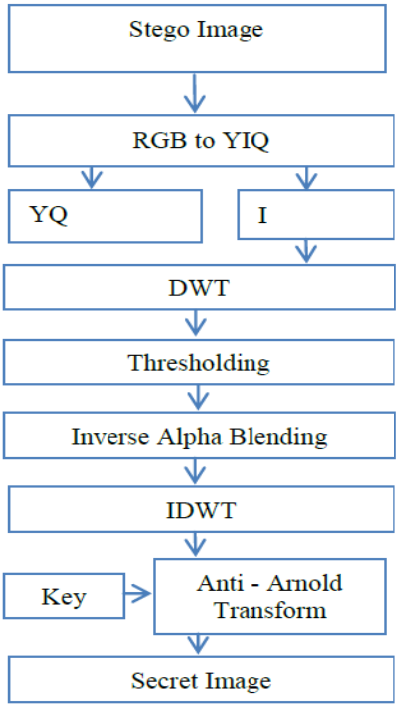

Fig.2 Block diagram of Proposed Method (Decoding).

A set of images of size 512*512 are used for experimental test as original cover image. Images are collected from databases such as SIPI and University of Washington. First the proposed scheme applied in applied in DWT domain. Testing the above method to fifty sets of images. Find out that PSNR value and MSE value are tolerable and hence acquire acceptable security and imperceptibility.

In Figure (3) shows the Proposed Method in case of DWT, cover image of size 512x512 shown in Figure 3.(a) and secret image or payload of size 256x256 shown in Figure 3.(b). Figure 3.(c) is the output obtained from Arnold Transform, Figure 3.(d) and 3.(e) shows the Stego image and recovered image respectively. The Final recovered Original image is shown in Figure 3.(f). In Figure(4) shows the Histogram test of DWT 4.(a) and 4.(b) shows the Histogram of cover and stego image.

The performance of PSNR ratio after the various attacks is shown Table I .We can reconstruct better secret image even after the Salt and Peeper, Gaussian ,speckele and Blurred attacks.

III. Results and Discussion

Fig. 3 Experimental result in case of DWT (a). Cover image (b) Secret image (c) Scrambling of Secret message (d) Stego image (e)Reconstruction of Secret, (f) Original Secret Message.

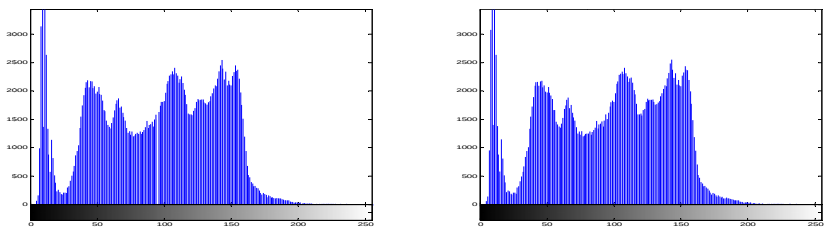

Fig. 4 Histogram result in case of DWT (a).Cover image, (b). Stego image.

TABLE I. THE PERFORMANCE OF PSNR AFTER ATTACK

Attacks	PSNR (Cover,Stego)
Salt & Pepper (0.0001)	48.3472
Gaussian G=0,h=0.000001	51.2711
Speckle G=0.000001	61.5831
Blurred H=Disk,0.5	61.5831
Sharpened (un)	29.2828
Scaling (10)	49.1539
Rotation (-0.0001)	31.1597
Rotation (+0.0001)	31.6834

TABLE II. THE PERFORMANCE OF QUALITY METRIC FACTORS IN DWT DOMAIN

Cover (512x512)	Secret (300x300)	MSE	PSNR	NCC	SC	NAE
Sunset	Sunflower	0.045	61.58	1.00	0.99	0.0004
Lavender	Sunflower	0.097	58.27	1.00	0.99	0.0008
Desert	Sunflower	0.103	57.99	1.00	0.99	0.0009
Azul	Sunflower	0.101	58.08	1.00	0.99	0.0008
Sunset	Hum	0.004	71.96	1.00	1.00	0.0004
Lavender	Hum	0.039	62.27	0.99	1.00	0.0003
Desert	Hum	0.066	59.91	1.00	0.99	0.0006
Azul	Hum	0.117	57.44	1.00	0.99	0.0009

The some of the image quality measurement has been calculated and corresponding tested results are shown in the Table II. It is observed that the better quality of stego image formed by the other image quality metrics followed in the ranges. PSNR value ranges from 58 to 72db. Both the NCC and SC are observed ranges from 0.99 to 1.00. NAE is observed from 0.0003to 0.0009.

IV. Conclusion

This paper presented a novel Secret writing methodology that utilizes 2D wavelet transform and image noise removal techniques. This process provides a method for concealing a digital data within a color cover image by adjusting a threshold value from noise removal methods to propose a high payload (capacity) with very little effect on statistical properties. In this Secret writing system the both cover image and secret data are decomposed into 2 level of wavelet decomposition. By applying a threshold which is calculated from detail coefficients of cover image, embedding points are detected and filled by normalized DWT coefficients of secret message. Experimental results shows that this proposed system gives the high security and capacity. As future extension, It is used to enhancing capacity and PSNR rate by level dependent denoising methods.

REFERENCES

[1] Ashish Chawla & Pranjal Shukla, "A Modified Secure Digital Image Steganography based on Dwt using Matrix Rotation Method", International Journal of Computer Science and communication Engineering, vol 2, pp 20-25, 2013.
[2] H S Manjunatha Reddy & K B Raja, " Wavelet based Non LSB Steganography", International Journal of Advanced Networking and applications, vol 3,issue 3, pp 1203-1209, 2011 .
[3] M. Ravi Shankar Reddy et al., 2013, "A Novel Method for Steganography in Spatial Domain",International Journal of Advanced Research in computer Science and Software Engineering, vol 3, issue 10.
[4] Wu S, Huang J, Huang D, Shi YQ: Efficiently self synchronized audio watermarking for assured audio data transmission. IEEE Transactions on Broadcasting 2005,51(1):6976, 10.1109/TBC.2004.838265.
[5] Lee SJ, Jung SH, A survey of watermarking techniques applied to multimedia. Proceedings of the IEEE International Symposium on Industrial Electronics, June, 2001, Pusan, South Korea 1: 272277.
[6] Kumsawat P, Attakitmongcol K, Srikaew A: A new approach for optimization in image watermarking by using genetic algorithms. IEEE Transactions on Signalrocessing 2005, 53(12):47074719.
[7] Sriyingyong N, Attakitmongcol K: Waveletbased audio watermarking using adaptive tabu search. Proceedings of the 1st International Symposium on WirelessPervasive Computing, January 2006, Phuket, Thailand 1: 15.
[8] Attakitmongcol K, Hardin DP, Wilkes DM: Multiwavelet prefilters—Part II: optimal orthogonal prefilters. IEEE Transactions on Image Processing 2001, 10(10):14761487.10.1109/83.951534
[9] Bibi Isac, Santhi, "A Study on Digital Image and Video Watermarking Schemes using Neural Networks", International Journal of Computer Applications (0975 – 8887), Volume 12– No.9, January 2011.