A SECURED IMAGE COMMUNICATION WITH DUAL ENCRYPTION AND REVERSIBLE WATERMARKING

Surya Boppanaa, William Kane, and Long Ma

Department of Computer Science, Troy University, Troy, Alabama, USA

ABSTRACT

Secured communication is the optimal means of exchanging information without the risk of data leakage. Data encryption serves as a crucial method for safeguarding and fortifying sensitive information. This paper introduces a groundbreaking approach known as reversible information concealment, specifically designed for digital images. It employs an integer-to-integer wavelet transformation alongside a companding process to embed and retrieve confidential data, restoring the image to its pristine state. Furthermore, the paper explores the utilization of genetic operators in cryptography. Given the prevalence of general information tampering within networks, it becomes imperative to protect messages during transmission. To address this concern, the paper proposes a novel encryption technique leveraging genetic operators such as crossover and mutation. This method ensures message confidentiality during the transmission process, contributing to an enhanced and more secure environment. The overarching goal is to establish a robust security framework through the integration of encryption and digital image watermarking for discreet data concealment within images.

KEYWORDS

Genetic Algorithm, Cryptography, Adaptive Thresholding, Companding Technique, Integer Wavelet Transform, Reversible Watermarking work Protocols

1. INTRODUCTION

Secured communication is achieved when two corresponding entities maintain no exposure, a pivotal factor in our contemporary lifestyle where data transmission serves as the linchpin for numerous societal functions. Acknowledging the profound impact of this interconnection, the imperative of securing data takes center stage as a primary technological responsibility. Tackling this challenge involves the strategic application of encryption to restore the original, un-watermarked image—an indispensable process highly valued in document imaging services catering to diverse enterprises. A related facet is cryptography, ensuring exclusive access to encrypted information for understood and predefined authorized users. Cryptography establishes qualified security across federal, economic, and social network domains [1]. Integrating these functions guarantees comprehensive, state-of-the-art image security, facilitating optimal utilization.

Watermarking in a digital image serves to obscure and safeguard encoded data linked to the original documenter, ensuring comprehensive accreditation. However, issues often arise, particularly with complex documents, where the original shape becomes distorted during the data installation phase. Mitigating this challenge proves challenging due to various factors such as bit substitution, quantization, and truncation. While some models acknowledge these struggles,

David C. Wyld et al. (Eds): ICCSEA, NLAI, SCAI, CSIA, IBCOM, SEMIT, NECO, SPPR, MLDS -2023
pp. 277 - 285, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.132421

certain fields, including medical and military enterprises, cannot afford such inaccuracies. Inconsistencies may lead to legal troubles, altering the perception of a doctor's findings or causing diplomatic and physical consequences for military maps. Reversible watermarking offers a solution in such scenarios, securely and accurately encoding and displaying a digital document with its original intent intact. A genetic algorithm [3] is a heuristic search based on natural hypothesized selection. This algorithm has five stages, which consist of three critical operators. These key functions are understood as population generation, crossover, and mutation. To kickstart this process is population generation, which brings about communicated binary or hex chromosomes for the introduction. The crossover phase is concerned with applying the operator of the same name to people in their current state to result in a parent solution. A mutation process is incorporated to achieve genetic diversity across species using a mutation director to achieve a fixated genetic standard. Some research has been done in this field as in 2012, Ankita Agarwal presented an encryption method that pairs the highlighted genetic algorithm with a genetic operator to achieve a fulfilled encrypted secret key image [4]. With research continuing in 2014, Sindhuja K and Pramila Devi S proposed a method to encrypt data using the operator's right shift, matrix addition, modulo operation, and genetic modifiers [5]. While advancements have been made in completely reversing a watermark on an image, in 2011, N.A. Memon brought about a stable method for showing the opposite hand of clear-cutting a watermark for an image [16].

This study introduces a strategic approach to reverse watermarking digital images using cryptography and paired algorithms for enhanced security and noise reduction. The outcome is a digitally watermarked image of superior quality and reliability. The work employs genetic operators and encryption methods in cryptography to fortify data movement. The PSNR block calculates the peak signal-to-noise ratio between two images, serving as a quality measure. MATLAB, a versatile numerical-performance language, is utilized for its computational, visualization, and programming capabilities. Our proposed method utilizes two-dimensional images for increased reliability. Digital image watermarking conceals information about the content creator or owner for authentication or copyright protection. However, the standard limitation of distortion in the original image is addressed through decryption and reversible watermarking, ensuring lossless data transfer and recovery, particularly in medical images.

2. PROPOSED APPROACH

Our proposed methodology elucidates the principles of fixed threshold-based companding, encompassing the establishment of a threshold framework, watermark creation, and the seamless embedding of the watermark into an image. These fundamental components form the groundwork for achieving reversible watermarking and adeptly concealing data within the target image. Each block within this process encounters an adaptive resolution of limits, strategically crafted to incorporate thresholds specific to individual blocks. The subsequent section provides a comprehensive breakdown of the constituent elements in our approach:

2.1. Fixed Threshold-Based Companding

Companding is the method of compressing a signal followed by extending said signal. Let Y be a compression function and X be an expansion function. For a signal f, Y and X have the accompanying relationship: Y(X(f)) = f. For a digital signal, Y_q and X_q represent the quantized versions for Y and X individually, and q indicates the quantization work. The compression function Y_q is given by [16]:

1. $$f_q = Y_q = \begin{cases} f & |f| < TH \\ sgn(f) \times ([|f| - TH/2] + TH) & |f| \geq TH \end{cases}$$

where sign(.) is the sign function, and TH is a pre-defined fixed threshold. The expansion function Y_q is given by:

$$2. \quad Y_q(f) = \begin{cases} f & |f| < TH \\ sgn(f) \times (2|f| - TH) & |f| \geq TH \end{cases}$$

Companding values via equations (1) and (2) produce expected results if | f | < TH. However, when | f | ≥ TH, the companding error is produced:

$$3. \quad z = |f| - |x_q(y_q(f))| \quad \text{where } Z \in \{0,1\}$$

A structured understanding of the Companding watermarking technique is as follows:

1) Compression function Y is applied to the original signal f to obtain a new signal $l = Y(f)$. Assume the binary expression of l is $p_1 p_2 \ldots p_n$, where $p_i \in \{0,1\}$.
2) A bit b $i \in \{0,1\}$ is appended after the least significant bit (LSB) of l. In this way, l becomes $l' = p_1 p_2 \ldots p_n b$ which can mathematically be expressed as: $l' = 2 \times l + b$.
3) In the data extraction stage, we only need to extract the LSB bit from the received signal h', which means b = LSB (l'). The signal l can thus be recovered by the expression $l = l' - b/2$.
4) After obtaining the signal h, we can recover the original signal by expression $f = Y_q(l)$ + Z, where Z is a companding error.

2.2. Watermark Creation

The prospective method creates the watermark from the following segments.

2.2.1. The Error Vector (Z)

If the coefficient estimation is more unique than or equivalent to the client-characterized limit, it is compressed (equation 1) and extended upon (equation 2). To have the capacity to recoup the first picture precisely, it is vital to gather the companding mistakes (equation 3) to recoup the entirety of the first picture. These mistakes are aggregated in vector Z [16].

2.2.2. Payload (P)

The payload can be defined as the communication to client characterized data, which can be any amount of mystery data identified with a picture [16].

2.3. Embedding Watermark into an Image

Partitioning the info picture understood as "I" into squares of size S × S. Figure the 2D IWT (Integer Wavelet Transform) of each block$^{(i,j)}$ up to level 2 [16]. Acquire the threshold T$^{(i,j)}$ from THMAP for the corresponding block$^{(i,j)}$ and therefore, apply the compression function on the coefficients of each sub-band (HL1, LH1, HH1) given the limit TH$^{(i,j)}$. Thus, implant the watermark W into a block$^{(i,j)}$ utilizing condition l' = 2 × l + b. and figure backward IWT to get the watermarked block'$^{(i,j)}$. The operation proceeds until the point where W is installed is put into the blocks, and THMAP should be embedded in the picture to facilitate active recovery. This action is performed because the embedding has been drawn out in each block with an alternate edge, which leads to TMAP being compressed and utilizing math encoding to decrease its size

fundamentally. Finally, compacted THMAP is embedded in level 2 coefficients (HL2, LH2, HH2) regardless of blocks using THMIN as well as other data implanted alongside THMAP as the extent of block, i.e., S. The stamped picture "I" in this manner acquired is the last watermarked picture.

Author names are to be written in 13 pt. Times New Roman format, centred and followed by a 12pt. paragraph spacing. If necessary, use superscripts to link individual authors with institutions as shown above. Author affiliations are to be written in 12 pt. Times New Roman, centred, with email addresses, in 10 pt. Courier New, on the line following. The last email address will have an 18 pt. (paragraph) spacing following.

2.4. Watermark Extraction

Process 2D IWT of image 'I' engages with the CDF channels and breaks down the image to level 2 to get HL2, LH2, and HH2 wavelet sub-groups. Demanding the realized threshold estimation of TMIN extract as the figured TMAP and data utilization of in the relation b = LSB (l'). Uncompressed TMAP-related data to discover TMAP and square size will lead to introducing B with block-size data. Separation of the watermarked image "I" into S × S measure blocks. Presently the process of the IWT of each block'(i,j) what's more, perform disintegration up to level 1, and for each block (i,j) , locate the corresponding threshold T(i,j) from THMAP. Concentrate the watermark from the wavelet coefficients of each block utilizing b = LSB (l') and collect all slightest significant bits utilized before recuperating the watermark bitstream W'. Decompress the bitstream W' utilizing mathematical unraveling calculation to restore the first-bit stream, and when "W" has been decompressed, the blunder vector Z' and payload P' can be recovered to form. Next would be restoring coefficients by utilizing condition, $\mathrm{l} = l' - b/2$ and getting the first coefficients by acting on the condition $f = {}^{Y_q}(h)$ + Z. The first picture is then acquired by taking the backward IWT of reestablished coefficients.

2.5. Creating Threshold Outline (THMAP)

Each block threshold can have its underlying details checked through the proposed method ahead of the actual watermark. To find the THMAP which is embellished as pursues is to use a block graph as follows: Introduce THMAP to an (M/S) × (N/S) zero framework, as S is the client characterized in the size of the block and M and N are the tallness and broadest of the info picture individually. Instate THINIT, THMIN, and PSNRMAX (Peak Signal to Noise Ratio) with the client-characterized values and set the estimation of TH as THINIT. Apply the compression work utilizing equation (1) on all parameters, even on vertical and slanting sub-band coefficients that are not as much as TH. Next, install the watermark in all sub-band coefficients independent of TH utilizing the equation l'= 2 × l + b, where l speaks to the first coefficient while b is the watermark bit to be implanted. Process the converse IWT of the block(i,j) to get block'(i,j) where I, j are line and section files of a block individually. [16] The PSNR of block*(i,j) is figured on the possibility of being malleable. If PSNR is observed to be more prominent or equivalent to the most extreme permitted PSNRMAX, the limit TH is recorded in THMAP. Presently decline the estimation of TH by one and this decrement in TH will increment the PSNR of the block in the wake of embedding the watermark. This is because of the way that when TH is little, to an ever-increasing extent coefficients are companded, and in this manner, installing twisting will be negligible, and the excellent visual nature of the stamped picture is accomplished. The emphasis will proceed till TH is equivalent to THMIN; thus, we obtain the lattice THMAP containing edge estimations of each block of information picture depending upon the properties of that block [16].

3. A SECURED PLATFORM

A comprehensive MATLAB tool consolidates all necessary components onto a unified platform, offering a seamless representation of complete information transmission with the added security of a Graphics Processing Unit (GPU) or a graphical user interface.

3.1. Watermarked Image Encryption

Textual data is given a designated space where it will undergo encryption. An image is selected to employ encrypted textual data. Here, the encrypted data is embedded into the image through the watermarking method. At last, this watermarked image will again go through another image encryption. Therefore, the encrypted image with hidden encrypted textual data will be transmitted to the desired destination.

3.2. Decryption and Data Recovery

The watermarked encrypted image is selected to wrest the image and data. Initially, the image is decrypted, and the original image is extracted through a reversible watermarking method. Now, the encrypted textual data is extracted from the image. The decryption process takes place using a key, which is generated during the time of encryption. At the time of decryption, selection of this key to decrypt the data. Therefore, we can see the original textual data that is transmitted originally.

This proposed approach is calculated only for the textual data. If any numerical data is brought into the equation, it will generate an error. Therefore, no numerical data is to be used in this approach. Figures 1 and Figure 2 are examples of the above-written data.

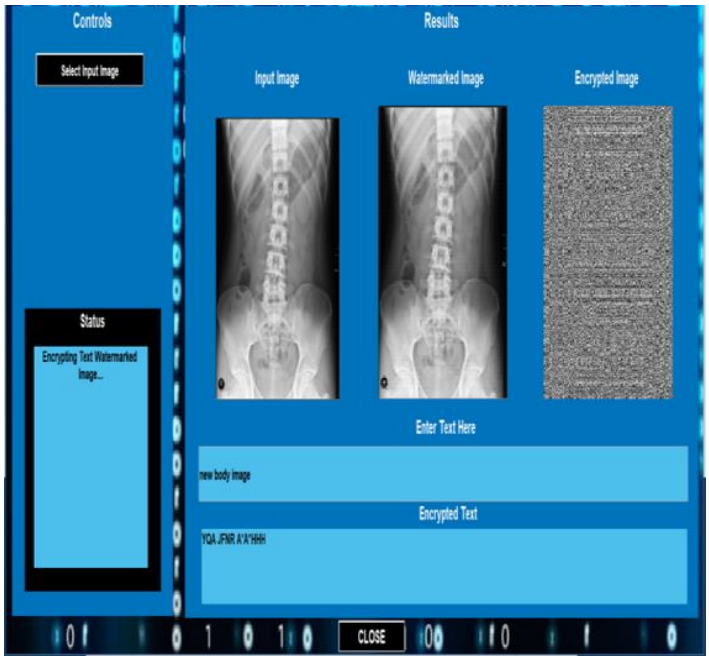

Figure 1. Embedding text and Encrypting the Image

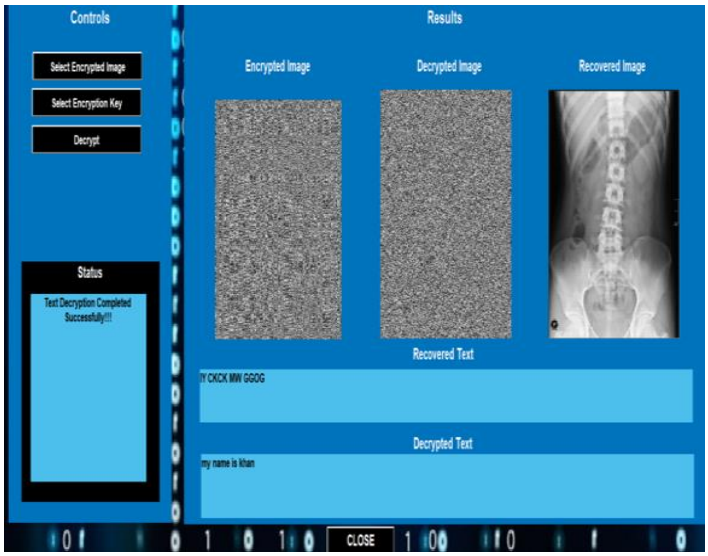

Figure 2. Decryption and extracting the original textual data

3.3. Recovery of Original Image

The following steps recover the original image:

1. Read the watermarked image I'
2. Iteration begins
3. Divide the watermarked image I' into blocks of size S × S
4. Compute the 2D IWT of a block (i,j) *using CDF filters (Cohen, Daubechies, Feauveau) and decompose it up to 2nd level*
5. Recover the coefficients by using $l = l' - b/2$
6. Expand the coefficients by using
7. $Y_q(f) = \begin{cases} f & |f|<TH \\ sgn(f) \times (2|f| - TH) & |f|\geq TH \end{cases}$
8. The first-level coefficients are expanded by using threshold $T^H(i,j)$ *and second-level coefficients with THMIN*
9. Obtain the original coefficients by adding the companding errors in recovered coefficients using f = $Y_q(h)$ *+ Z.*
10.. Compute the inverse IWT to get the original block(i,j)
11 .Iteration ceases
12. The process will be continued until all the blocks are processed. Therefore, the resultant image will be the same as the original image

4. EXPERIMENTAL RESULTS

Our experiment uses standard 2D pictures of X-ray, CT scan, Ultrasound, and MRI with size 512 × 512. The first encrypted and watermarked adaptations of these pictures appear in Fig. 1, and the settled qualities of THMIN and PSNRMAX are heuristically set to 2 and 42.0 dB separately. Be that as it may, the estimation of THINIT is chosen in the scope of {2-15}. The value of PSNRMAX can be divided according to a requested dimension of imperceptibility utilized in a specific application. The evaluation of PSNRMAX straightforwardly controls the nature of the watermarked picture. For watermarked pictures appearing in Fig. 1, the initial threshold (THINIT) is 15, and the block size is set to 8 × 8.

The suggested technique grants improved ambiguity regarding the PSNR for a similar payload. This area of enhancement is prominent at low- and high-level payloads. The distinction or enhancement is more if there should be an existence of finished pictures. This claims the installation is performed on high recurrence, which gives an abundance of inserting space in finished pictures and is utilized by the nearby limit adjustment. Altogether, we connected every one of the strategies into one stage with a GUI in which we can take the necessary steps from encryption of literary information, watermarking of pictures, information inserting, and encryption of printed information as every yield will be unmistakable on a similar GUI screen.
Therefore, in Fig. 3, we can see the original image and watermarked images with embedded textual data, including encrypted images and encrypted textual data. Following this, we can send a message through the encryption and watermarking process to send the data. At the same time, we can decrypt the same message by extracting the original image from the watermarked image, resulting in the finalized uncovered image. Fig. 4 displays the comparative results of X-ray images for different block sizes.

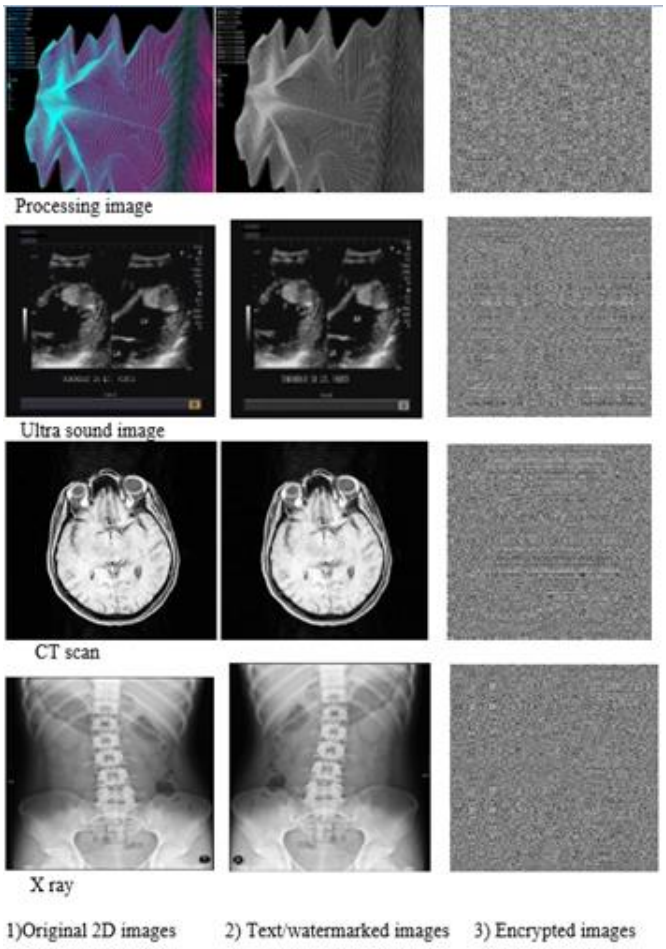

Figure 3. Types of 2-Dimensional Images with Watermarking and Encryption

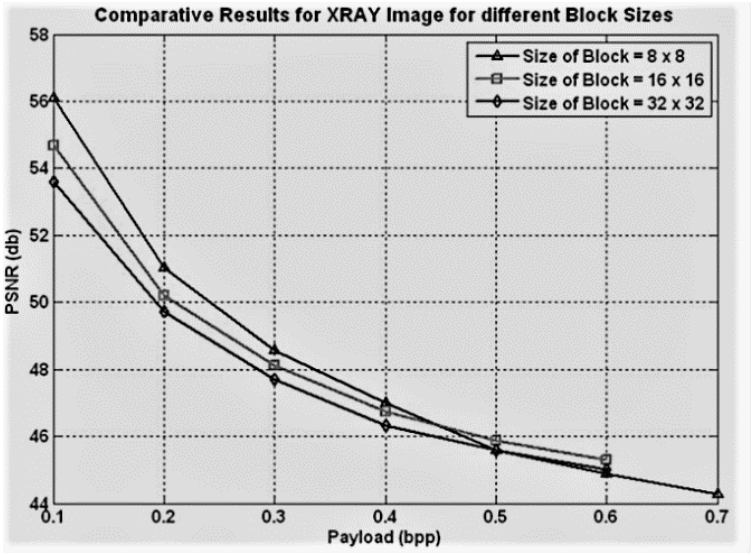

Figure 4. Results of X-ray images on different block sizes

5. CONCLUSIONS

This paper introduces a straightforward cryptographic framework employing genetic algorithm operators for encryption, ensuring robust security. The incorporation of frequent binary and decimal transformations enhances its overall capability. The suggested reversible watermarking system, reliant on companding and adaptable thresholding, exhibits potential applications in image comparison within military, medical, and law enforcement domains. The approach involves block-based watermarking and iterative threshold progression to uphold histogram quality efficiently. The method ensures secure data coverage, rendering transactions impervious to external threats, making it versatile across diverse industries. Additionally, it can be customized to integrate both textual and numerical data. This conceptual development has the potential for extension into the realm of artificial intelligence, offering a reduction in data transfer time complexity.

REFERENCES

[1] Behrouz A. Forouzan, Cryptography & Network Security—, Tata McGraw – Hill, 2007.
[2] William Stallings, Cryptography and Network Security‖, 3rd Edition.
[3] S., N. Sivanandan, S. N. Deepa, Introduction to Genetic Algorithms, Springer Verlag Berlin Heidelberg, 2008.
[4] Ankita Agarwal, ―Secret Key Encryption Algorithm Using Genetic Algorithm‖, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012.
[5] Sindhuja K, Pramila Devi S, A Symmetric Key Encryption Technique Using Genetic Algorithm‖, International Journal of Computer Science and Information Technologies, Vol. 5 (1 2014).
[6] Amritha Thekkumbadan Veetil, An Encryption Technique Using Genetic Operators, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 4, ISSUE 07, JULY 2015
[7] S. Hai-mei, M. Tian-can, Q. Qian–ging, "Spread Spectrum Watermark based on Wavelet Transform for Still Digital Image," *Wuhan University Journal of Natural Sciences*, vol 9, No. 2, pp. 203-208, 2004.
[8] A. Khan, A.M. Mirza, "Genetic perceptual shaping: utilizing cover image and conceivable attack information during watermarking embedding, Information," *Fusion*, vol. 8, pp. 354-365, 2007.
[9] A. Khan, "Intelligent perceptual shaping of a digital watermark." PhD Thesis, Faculty of Computer Science and Engineering, GIK Institute, Pakistan, 2006.

[10] J. H. K. Wu, R.F. Chang, C. J. Chen, C. L. Wang, T. H. Kuo, W. K. Moon, W. K. Chen," Tamper detection and recovery for medical images using near-lossless information hiding technique," Journal of Digital Imaging, vol. 21, no. 1, pp-59-76, 2008.

[11] N. A. Memon, S.A.M . Gilani, " NROI watermarking of medical images for content authentication," In the Proceedings of 12th IEEE International Mutitopic Conference (INMIC'08), Karachi, Pakistan, 2008. p. 106- 110.

[12] S.I. Fraser, A.R. Allen," A high capacity reversible watermarking technique based on difference expansion," In the Proceedings of Signal and Image Processing, Kailua-Kona, HI, USA, 2008.

[13] J. Tian, "Reversible watermarking by difference expansion," In Proceedings of Workshop on Multimedia and Security, 2002. p. 19-22.

[14] G. Xuan, Y.Q. Shi, C. Yang, Y. Zheng, D. Zou, P. Chai," Lossless data hiding using wavelet transform and threshold embedding technique," Proceedings of IEEE International Conference on Multimedia and Expo, 2005. p. 1520-1523.

[15] G. Xuan, C. Yang, Y. Zhen, Y.Q. Shi, Z. Ni," Reversible data hiding using IWT and companding technique," I. J. Cox et al. (Eds.) IWDW 2004, LNCS 3304. p. 115-124. World Academy of Science, Engineering and Technology 55 2011 620.

[16] Nisar Ahmed Memon, A Novel Reversible watermarking method based on adaptive thresholding and companding technique, World Academy of Science, Engineering and Technology 55 2011