Image Steganography Using Integer Wavelet Transform and Secure Using Arnold and Chaos Based Encryption

[1]Shweta Tiwari, [2]Varsha Sharma

[1]M. Tech, Information Technology
[1]RGPV, Bhopal, India

***Abstract*— Steganography is the science and art of writing hidden information details in a way that no one apart from the sender and intended recipient even realizes there is hidden information. In this proposed algorithm is a Steganography method based on Arnold transform and Integer Discrete Wavelet Transform (IDWT). In this paper arithmetic encoding technique is used to enhance the capacity of the steganography. The second level decomposition Integer wavelet transformation is accessed to transform the image into its wavelet domain. The chaos sequence is used in the paper for the proving the encryption. The proposed method achieved high security and more imperceptibility.**

***Index Terms*— Steganography, Integer Wavelet Transform (IWT), Arnold Transform, Chaos Transform Embedding, etc.**

I. Introduction

The ultimate objectives of Steganography are robustness, un-detectability, and enhanced hidden data capacity. These are the main features separating it from related schemes of watermarking and cryptography. Digital watermarking is the way of concealing a message related to the digital signals i.e. either video or an image or song within the signal itself. Watermarking hides the message relating to the actual content of the digital signal whereas in steganography there exists no relation between digital signal and actual message. The digital signal is only used as a cover to hide its existence. Since Media files are large in size, steganography is ideal for their transmission as it provides more security with ease. In digital steganography, steganographic coding is done at the transport layer for electronic communications.

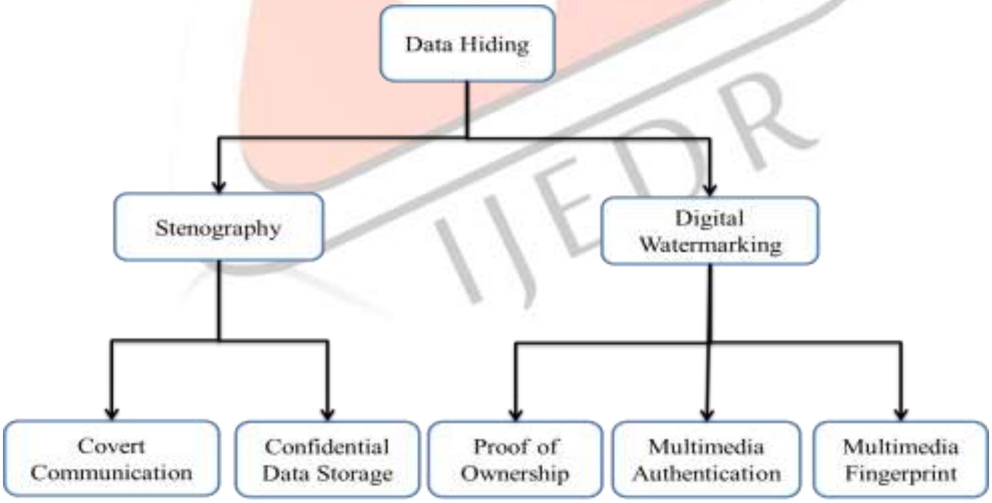

Figure 1 Classification of Data Hiding process

II. RELATED WORK

W Many researchers have been done significant work in the field of watermarking techniques Based upon different wavelet transform problem; some of the work is described in this:

M. A. Ghonemy et al., [1] presented Wavelet transforms mapping integers to integers allowing perfect reconstruction of the original image. He proposed an algorithm for embedding the message bitstream into the LSB's of the integer wavelet coefficients of a true-color image. The algorithm also allows step of pre-processing on cover image to adjust saturated pixel components for recovering the embedded message without loss.

Gautom Sanyal et al., [2] proposed innovative approach of developing secure steganography of image based model using IWT. The corresponding experimental results show the integrated approach of combining IWT, modified LSB and segmentation techniques enabling secure transfer.

Parul, et.al, [3] in paper presented new perspective for image steganography with the help of DWT. In this approach, the cover image gets divided into sub-bands of higher and lower frequency and data has embedded into higher frequency sub-bands. To enhance the security of the message Arnold Transformation is utilized. The suggested approach has been implemented in MATLAB 7.0 and the performance is evaluated on the basis of capacity, PSNR and correlation. The proposed approach resulted in higher capacity in embedding of image steganography when compared to other existing ones.

Poonam H. Mahajan, et.al, [4] used the fusion of DWT-DCT Transformation for digital image watermarking. This fusion technique exhausts caliber of 2 methods in frequency domain; DCT and DWT, to achieve better physical property and robustness. The idea is based on the predicament that new method may eliminate the drawbacks of available watermarking approaches. The joint approach resulted in associate elective watermarking methodology. Another powerful method is suggested in paper which is the fusion of. This new algorithm removes the random sequences as generated by Arnold and Chaos transformations. To hide image into frequency domain, third level decomposition of ripple transformation is employed separately. The combination of Blind Digital Image Watermarking mistreatment DWT and twin coding Technique is proved to be more efficient.

III. Watermarking Techniques

The Digital watermarking schemes are classified into two domains: pixel domain or spatial domain and transform domain or frequency domain.

In this frequency domain technique, watermark is directly embedded by amending pixel values of host image/video file. The foremost advantages of scheme based on pixel are that they are simple conceptually with very low computational intricacies. These techniques commonly exploits in watermarking video process with real-time performance as prime concern. The watermark in resulting process may perceptible or may not be perceptible. The perceptibility lies on intensity value. As instance picture cropping used commonly by image editors, can be employed to remove the watermark. Some techniques for watermarking in spatial domains are Correlation based techniques. In these schemes, watermark data W(x, y) is get added to original content O(x, y) as per equation (1).

$$Ow\ (x,y)\ =\ O(x,y)\ +\ kW(x,y) \qquad (1)$$

In equation (1), k gives gain factor and Ow is watermarked content. As we increase the value k it will result in expense the quality of watermarked contents.

IV. Proposed Work

Nowadays LSB is trending as popular Steganography technique. Secret messages are hidden in the RGB image as per its binary coding. The secret messages are hidden with the help of LSB algorithm. Thus modifying LSB technique is proposed as the watermarking method to obtain same image quality as it is prior to encoding. The modified hiding process involves hiding of two bits by employing two bits by taking identical values which results in good quality of image.

Least Significant Bit Modification

Simplest approach in this domain is Least Significant Bit modification. This method embeds the watermark image by using the least significant bits of the original video or flips the Least Significant Bit (LSB). It is the most popular approach due to its simplicity, then yet with some limitations of dealing incompetence in range of attacks, poor quality of the produced video and least robustness and lack of imperceptibility.

Integer Wavelet Transforms (IWT)

The wavelet domain is now quickly growing. Many mathematical papers are being published monthly. Wavelets are utilized effectively in different diverse fields that includes approximation theory with signal processing, physics, astronomy, and image processing. One dimensional discrete wavelet transform is a repeated filter bank algorithm. The input is convolved with a high pass filter and low pass filter. The result of the convolution is a smoothen form of input and high frequency part is gathered by first convolution. The reconstruction inculpates convolution employing synthesis filters and the results of convolutions are added. In two dimensions, first step of one dimensional transform is applied to all rows then to columns. Further process is applied to the coefficients resulted from convolution in both directions. Figure 2, clears the above statements. The four classes of coefficients be: (HH) coefficients representing image diagonal features, (HG and GH) show vertical and horizontal information. At the last level, low pass coefficients (LL) are used. The same decomposition can be applied on the LL quadrant at range of log2 (min (height, width).

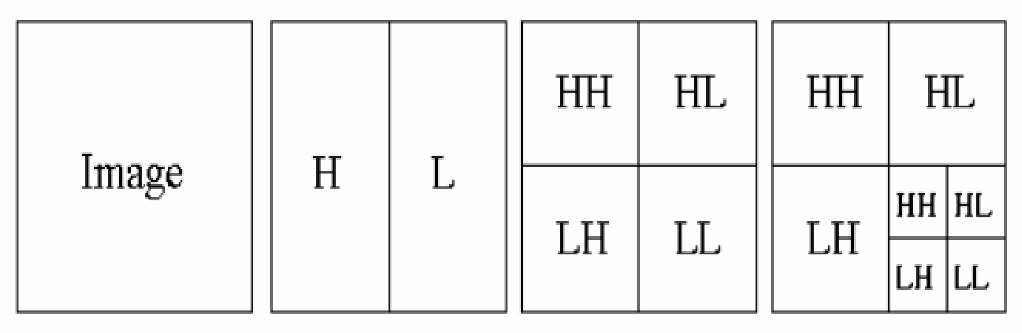

Figure 2 Two-Dimensional Wavelet Transform

As discrete wavelet transform works for independent processing of resulted components without perceptible interaction significantly between them, thus it makes process as imperceptible for effective embedding. The wavelet filters have floating point coefficients. When input data involves integers' sequences as in images, resulting filtered outputs contain no integers longer, which hinder perfect reconstruction of original image. But the Wavelet transforms map integers to integers; therefore it is introduced to characterize output with integers completely.

S-transform of wavelet transforms maps integers to integers. The smooth (s) and detail (d) outputs of S-transform for index n are respectively given in (2) and (3). The smooth and the detail outputs result on applying high-pass and low-pass filters respectively. At first instance, it makes vision of rounding-off of s(n) discarding little bit information. The sum and the difference of two integers are either both odd or both even. Therefore last bit can be omitted safely of the sum as it equals to that of difference. This makes S-transform reversible. The inverse S-transform is below given in equations (4) and (5).

$$s(n) = \left[\frac{x(2n)+x(2n+1)}{2}\right] \qquad (2)$$

$$d(n) = x(2n) - x(2n+1) \qquad (3)$$

$$x(2n) = s(n) + [d(n) + 1/2\,] \qquad (4)$$

$$x(2n+1) = s(n) - [d(n)/2] \qquad (5)$$

Arnold Transform

The Arnold transformation, also referred cat mapping, is a matrix changing tool from one into another. A be N X N matrix, a point i can be shifted to another point ï by equation:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} (mod\ N) \qquad (6)$$

Arnold transform system operates better encrypting images applications. For an N X N matrix image, Arnold transform is given by equation (6) where $(a, b\ )$ and $(x, y\ )$ express the pixel coordinates of the original and encrypted images, respectively. With the periodic boundary treatment, the image encryption using iterations of the Arnold transform may be written as:

$$I(x,y)^{(k)} = ID(a,b)^{(k-1)}(mod\ N) \qquad (7)$$

Where, $k = 1,2, \ldots N\ \ and\ I(x,y)0 = I(a,b)$. The Arnold transform matrix is given as in and I is an $N \times N$ image field. The encrypted image may be inverted by applying the inverse of the Arnold matrix times as follows:

$$I(a,b)^{(k)} = ID^{-1}(x,y)^{(k-1)}(mod\ N) \qquad (8)$$

Where, $(x, y)0$ refers to encrypted image pixel. After iterations, original image results as per the size of image given. The periodicity depends on the size of the images.

Followed by certain number of Arnold transformation, matrix A reappears. Number of Arnold transformation in which A reappears, is then denoted as period. In our experiments, Arnold transformation is performed on 128×128 matrices, and period=96. After Arnold transformation, security and robustness of our algorithm is get increased.

Chaotic Encryption

Chaos signals are dynamical, pseudorandom and irreversible signals possessing good pseudorandom sequences characteristics. Chaotic systems are sensitive highly to initial parameters. The output sequence show good randomness, correlation, complexity and is similar to context with white noise. Chaotic sequences possess linear complexity and non-predictability quite high. The 1-D Logistic chaos model is:

$$x(n+1) = \mu * x(n) * [1 - x(n)] \quad (9)$$

Where, μ ϵ (0, 4); x (n) ϵ (0, 1). By initializing μ and x (0), corresponding chaotic signal is formed. For yielding chaotic sequences, the chaotic signal x (n) needs to be transformed into binary sequence s (n). Therefore T[x (n)] is utilized as quantized function and can be given by.

$$T[x(n)] = \begin{cases} 0 & x(n) \in U_{k=0}^{2^{m-1}} \quad I_{2k}^{m} \\ 1 & x(n) \in U_{k=0}^{2^{m-1}} \quad I_{2k=0}^{m} \end{cases} \quad (10)$$

'm' is random integer and must be greater than 0. (I0m,…….) shows equal continuous interval in [0, 1] and the interval is divided by 2m . For value in odd interval of quantized function, the quantized value is 1 else quantized value is 0. The binary sequences generated would possess good pseudorandom sequence features. Chaotic key sequence are XORed by binary image, generated the encrypted watermark image.

V. Results

The performance of the IWT algorithm based digital image steganography using four cover images: Thumb impression, Lena, each of size 512× 512.

The various results are obtained after matlab simulation.

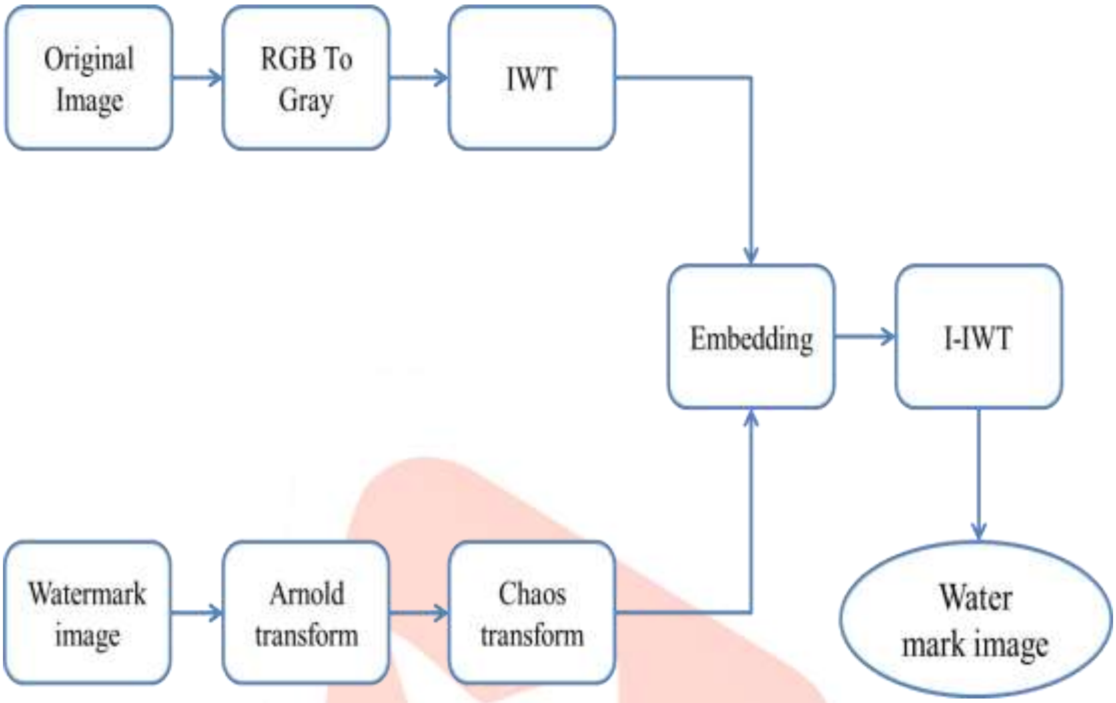

Figure 3 System Block diagram Water mark technique with IWT

- In proposed work we start by selecting two kinds of image one is for cover image and another is for watermark image.
- The RGB to gray converter.
- Here we apply IWT transform using only cover image. And the watermark image is applying Arnold transform and chaos transform.
- Now apply embedding algorithm.
- Combined watermark and cover image then, Apply Inverse level IWT transform.
- Calculate PSNR & MSE value for Embedding Process.
- The output results of watermark image.

Figure 4 Original Image of Lenna

Figure 4 shows the thumb impression before watermarking the image.

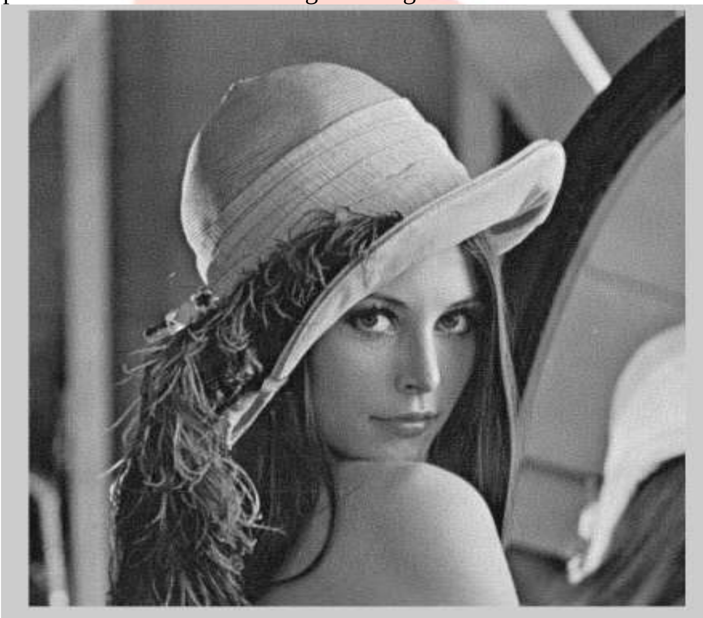

Figure 5 Watermarked image

TABLE. 1 Performance Parameter

Sr. No.	Specification	Value
1	Data size	126 k
2	PSNR	29.84
3	payload	0.34

Figure 5 represents the watermarked image in pixel domain. The image shows that pixels are added to the watermarked image to be embedded.

Figure 6 The Restored Image

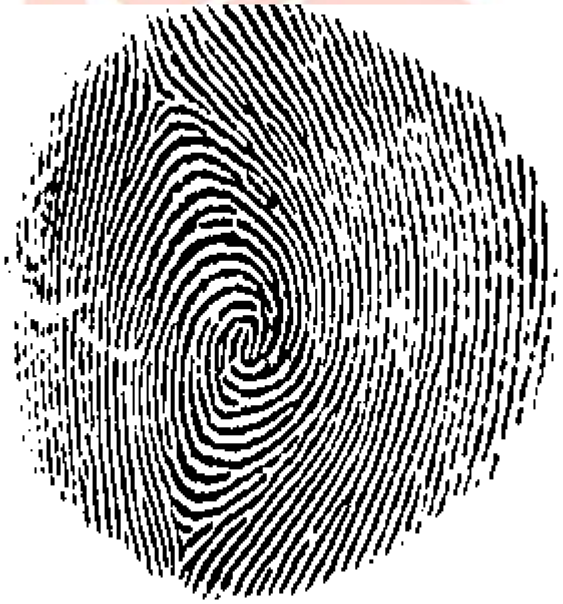

Figure 7 Retrieved Watermark Image

VI. CONCLUSION

The paper presented a new modified Steganography technique. The modified technique is then implemented and analyzed. The suggested scheme proves as an efficient method to hide the secret message depending over traversing of identical bits between image pixels values and the secret messages. The given method is compared with the LSB benchmarking method to directly hide the secret message in least two significant bits of image pixels. The suggested technique turned out as simple, more efficient, more accurate and appropriate than LSB method. The method first searches for identical values and procedure of hiding starts. Thus resolution of the image changes quite slowly which makes the secret message more secure.

REFERENCES

[1] M. F. Tolba1, M. A. Ghonemy, “Using Integer Wavelet Transforms In colored Image-Steganography” IJICIS Vol. 4 No. 2, July 2004.

[2] Poonam H. Mahajan, Pramod B. Bhalerao, “A Blind Digital Image Watermarking using Joint DCT-DWT and Twin Encoding Methodology”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-4 Issue-6, November 2014.

[3] Bhattacharyya S , Kshitij A P, “A Novel Approach to Develop a Secure Image based Steganography Model using Integer Wavelet Transform”, International Conference on Recent Trends in Information, Telecommunication and Computing,2010.

[4] Nidal F. Shilbayeh, Belal Abu Haija, "Combined DWT-CT Blind Digital Image Watermarking Algorithm", International Scholarly and Scientific Research & Innovation 7(6) 2013.

[5] Surya Pratap Singh, “A Robust Watermarking Approach using DCT-DWT”, International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 8, August 2012.

[6] Gursharanjeet Singh Kalra, Dr. Rajneesh Talwar, “Robust Blind Digital Image Watermarking Using DWT and Dual Encryption Technique”, Third International Conference on Computational Intelligence, 2011.

[7] Saeed K. Amirgholipour , Ahmad R. Naghsh-Nilchi, “Robust Digital Im-age Watermarking Based on Joint DWT-DCT”, Computer Engineering Dept, Isfahan University, IRAN, 2009.

[8] Thi Hoang Ngan Le, Kim Hung Nguyen, Hoai Bac Le, “Literature Survey on Image Watermarking Tools, Watermark Attacks, and Benchmarking Tools”, Second IEEE International Conferences on Advances in Multimedia, 2010.

[9] I. Cox, J. Kilian, F. T. Leighton and T. Shamoon, “Secure spread spectrum watermarking for multimedia”, IEEE Transactions on Image Processing, Vol. 6, Pages: 1673-1687, December,1997.

[10] Gursharanjeet Singh Kalra,Dr. Rajneesh Talwar, “Robust Blind Digi-tal Image Watermarking Using DWT and Dual Encryption Technique”, Third International Conference on Computational Intelligence, 2011,