Development of Secured 3-Level Wavelet Decomposition Steganography using Arnold Chaotic Map

Subodh Sharma[1], Prof. Angad Dixit[2]

[1]*Mtech. Scholar,* [2]*Research Guide*

Department of IT, NIIST, Bhopal

Abstract -Image watermarking is one of the security method applied to authenticate the digital images. The watermarking techniques were discussed has lots of advantage but single layer of security. So in this work we have designed an algorithm to increase the security of image watermarking, which will make watermarking more robust and even used to share secure data across devices. In this research for the embedding of secret information which was called as watermark image is a grayscale image which is being hidden behind cover image using three level discrete wavelet decomposition and for enhancing security secret or watermark image was encrypted with arnold chaotic map approach with a private key. This algorithm has advantage over previous algorithm because it has higher peak signal to noise ratio(PSNR) and structural similarity index(SSIM), which proves the robustness and ability information security as well as efficient watermarking system.

Keywords - Wavelet decomposition, multilevel decomposition, image steganography, security, chaotic map theory, encryption.

I. INTRODUCTION

In recent years, with the development of digital communication technology, computer network technology and information compression technology, information dissemination and access have become increasingly convenient and fast. Every user can easily download digital multimedia (such as images, audio, and video) files from the Internet. So piracy and copyright disputes have also become an increasingly serious problem.

Information that can be read and implicit without any special procedures or method is termed as plaintext or clear text. The technique of concealing plaintext in order to hide its particular material is called encryption. The impression of encryption is to make a message incomprehensible, except to the receiver.

Therefore, how to protect copyright and information security effectively has become a pressing practical problem. Traditional encryption techniques can simply guarantee the security of digital multimedia information during transmission; however, there are still some limitations to the protection of the integrity of digital multimedia content and the prevention of unauthorized copying. In this context, a supplementary encryption technology, digital watermarking technology has been proven an effective tool for copyright protection. The copyright protections of digital multimedia information through certification have been rapidly developed based on the watermarking technology.

Data encryption technology is used to benefit protection against loss, exploitation or alteration of private information. Encrypting plaintext results in indecipherable rubbish called cipher text. Encryption is used to guarantee the hidden information from anyone of concern not intended to, even those who can comprehend the encrypted data. The procedure of backsliding cipher text to its original plaintext is considered as decryption.

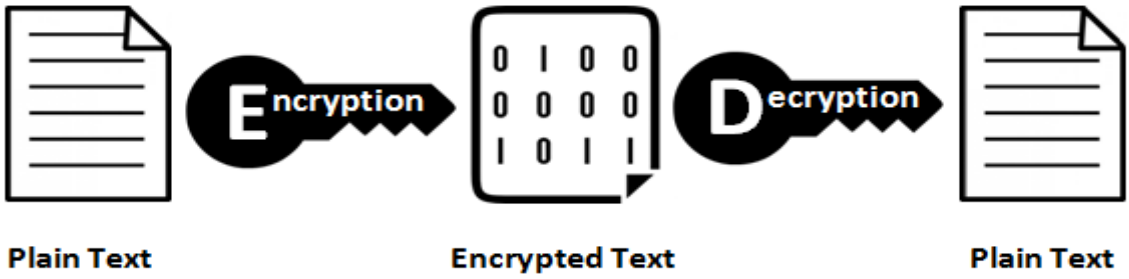

Fig. 1.1 Encryption and Decryption.

Digital watermarking, or digital tagging, could be data, serial numbers, characters, image symbols embedded with logo or copyright information, which contains the tag or code of the copyright holder, and can confirm legal

ownership of data and other information. Digital watermark can be secretly embedded into digital products to help identify the copyright, digital rights, and the integrity of the contents of these products.

The basic idea of digital watermark is embedding the secret information into the host, such as image, video, audio, text and software. In the context of protecting the copyright of a digital product, the technology has quickly become a hot concept for addressing the copyright protection problem in the emerging global digital network. A digital watermark needs to be properly changed and embedded into products. Therefore, the study of multimedia security algorithms is an imminent concern.

II. ENCRYPTION OF DIGITAL WATERMARKING

From image processing perspective, the embedded watermark signal can be treated as a weak signal superimposed in a strong background, as long as such superimposition of the watermark signal strength is below the human visual system (HVS) of the contrast threshold, that is, the existence of the signal is undetectable for humans. The contrast threshold is affected by the visual system of the space, time and frequency characteristics. Therefore, by adjusting the original image, it is possible to embed some information without changes in visual effects.

From digital communication perspective, watermark embedding can be understood as a narrow-band transmission signal transferred on a broadband channel (carrier image) by spread-spectrum communication technology. Although the watermark signal has certain energy, the energy distributed on any channel is hardly extracted to be detected. Watermark decoding (extraction of detection) is used to detect a weak signal from a noisy channel.

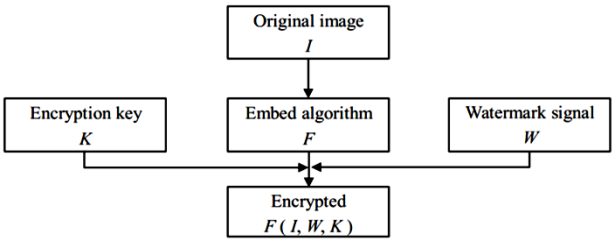

Fig. 2.1 The Watermark embedding process.

the watermark can be extracted accurately, which is called the watermark extraction process. As is show in figure 2.2, in the application of integrity confirmation, the embedded watermark must be accurately extracted in order to identify multimedia data integration by watermark integration verification.

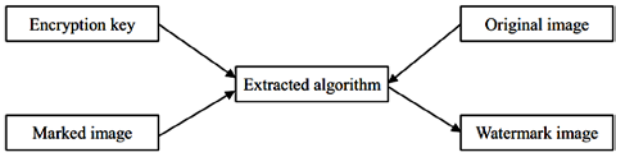

Fig.2.2 Watermark extraction process.

After undergoing these operations, the extracted watermark looks very different. Thus, a watermark detection process is needed. Refer to figure 2.3.

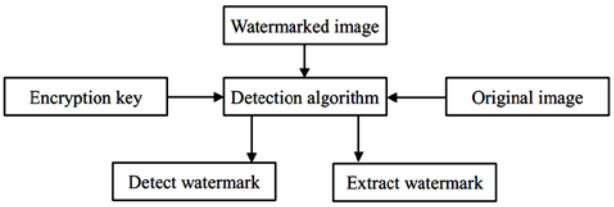

Fig.2.3 Watermark detection process.

III. PROPOSED METHODOLOGY

To ensure the security of digital image information, there are two effective protective measures. The first one is digital watermarking technology, which embeds a watermark in an entire image to effectively protect digital copyright. But this method is not able to change the appearance of an image, which is not suitable for the confidential needs of image. The other method is image encryption. Through encrypting operations of this method, the original image is transformed to information similar to channel random noise, and such random noise is not recognizable to people who do not have the encryption key. With the fast growth of networking technology, image encryption techniques have good application prospects. To enhance the performance and robustness existing of existing watermarking algorithm a new approach has implemented and simulated in MATLAB in this work. The proposed algorithm is a Secured 3-Level Wavelet Decomposition Steganography using Arnold Chaotic Map.

For encryption of image, traditional encryption algorithms are used to encrypt image. Based on the secret keys used in the processes of encryption and decryption, traditional encryption method can be divided into asymmetric-key cryptography (also known as secret key and public-key) and symmetric-key cryptography.

The image can be encrypted through conventional encryption techniques, but most traditional encryption technologies are based on text design without considering the inherent characteristics of images, thus the conventional approach is not only inefficient but less

secure. To overcome these problems, a 3-level wavelet decomposition steganography is used in this examination. Fig. 3.1 shows the block representation of proposed algorithm. To make proposed approach robust and secure following key concepts are used.

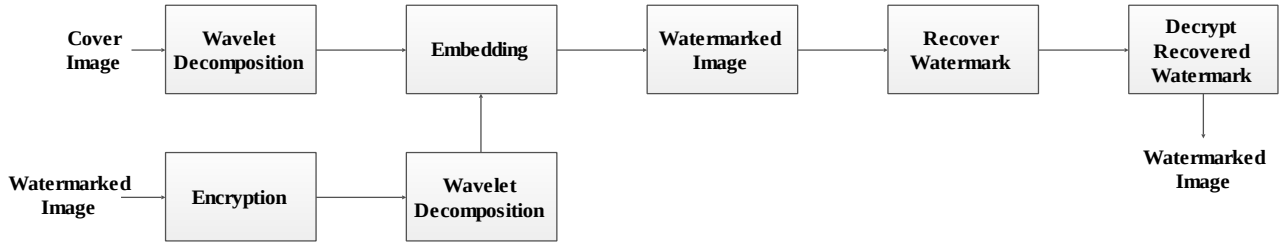

Fig.3.1 Block diagram of proposed work.

a. Arnold Transforms

The Arnold mapping is used in proposed approach to produce the chaotic sequence of watermark embedded. The Arnold transforms algorithm introduces the correct binary values of computing to embed watermark into deep image of wavelet domain in a low-frequency graph, and watermark detection does not require the original image.

It is a classical application of cryptography−the Caesar Cipher; which is based on the scrambling of position space and color space in digital image scrambling. The resulting image will be encrypted.

Arnold transform can be considered as stretching, compressing, folding and matching processes. Through these processes, discrete digital image matrix can be rearranged. Discrete digital image is a kind of finite set. The result of such transforms can cause chaotic of position changes of pixels.

b. Chaotic Cipher Algorithm

There are some basic properties in chaotic systems, such as certainty, ergodicity, and randomness. Combined with the concepts of confusion and spread of cryptography, these properties can be used to design cryptography algorithm, which forms chaotic cryptography. Chaotic cryptography is a multidisciplinary science that spans various fields, including chaotic theory, conventional cryptography, communication engineering, and information processing. Chaotic cryptography has two basic forms: the one is the simulation of chaotic security system that uses analog circuits and synchronization technology; the other one is achieved by digital circuits or computer digital chaotic cryptography, but it is not linked with chaotic synchronization. Studies of cryptographic systems show that most chaotic synchronizations of the communication systems have many flaws and breaches. In proposed approach in order to meet encryption a Chaotic Map is used.

C. Wavelet Decomposition

Wavelet decomposition is used to achieve better compression ratio image in proposed algorithm. Using wavelet decomposition multiple level decomposition could be achieved. A wavelet transform empowers to multi-resolution decomposition of image. Wavelet analysis provides decompose and reconstruct wavelet in easy manner motivated to apply wavelet decomposition in proposed approach.

The steps of flow of proposed algorithm in MTALAB platform has been shown in Fig.3.2.

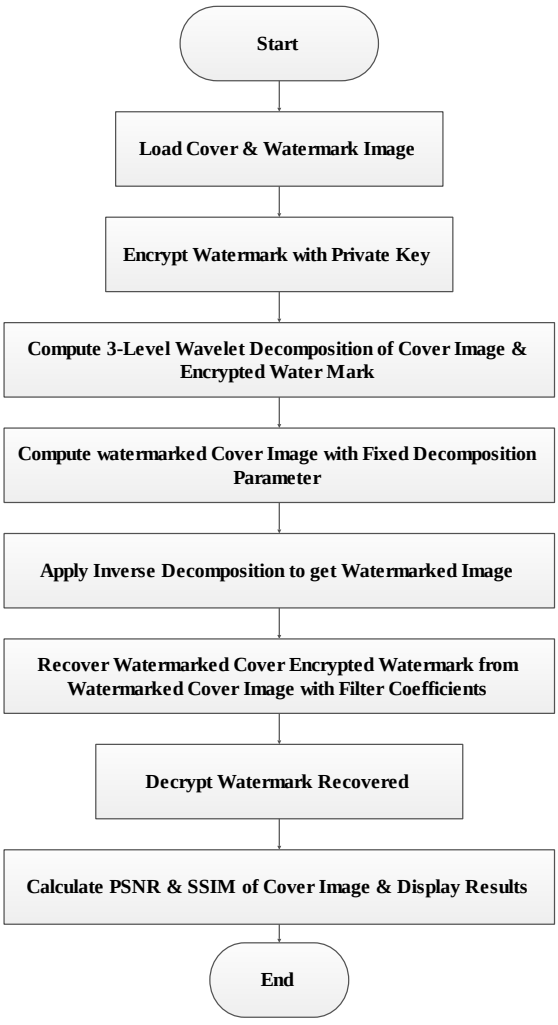

Fig.3.2 Flow Chart of proposed work.

IV. SIMULATION RESULTS

The Simulation of proposed algorithm has performed in MATLAB Simulation environment. The proposed algorithm combined with secured 3-level Wavelet Decomposition along with Arnold Chaotic map. This feature is suitable for image encryption. Simulation experimental and performance analysis of proposed algorithms are provided in following has been done with test cover image and watermark image.

The complete image encryption scheme consists of several steps of operation. First step is key generation, select a select a sequence of 128 bits as the key, and split them into n groups, which are further mapped onto to several parameters of the Chaotic map. The decrypted image is can be seem clear and correct by use the key.

These solutions can improve the unpredictability of encrypted images and are proven effective and feasible by various experimental analyses. An encryption algorithm is proposed to in this examination to process extra large-scale images, which expands the application of chaotic encryption.

In order to prove the universality of proposed image encryption approach, the selected images for the experiments were Peppers Cover Image and Lena Cover image is used as shown in Fig. 4.1 Peppers Cover image at top left is the original image and original flower watermark in to middle and encrypted watermark at top right shown in figure. The bottom right image in figure shows the decrypted watermark and the bottom middle image shows the recovered watermark and bottom right shows the watermarked image. These overflowed chaotic attractor lost the ability of encryption. Therefore the resulted image still maintains the feature of the original image, as shown in figure.

In figure Fig. 4.2 Peppers Cover image at top left is the original image and CHAOS image as a watermark in to middle image in figure and encrypted watermark at top right. The bottom right image in figure shows the decrypted watermark and the bottom middle image shows the recovered watermark and bottom right shows the watermarked image. These overflowed chaotic attractor lost the ability of encryption. Therefore the resulted image still maintains the feature of the original image, as shown in figure

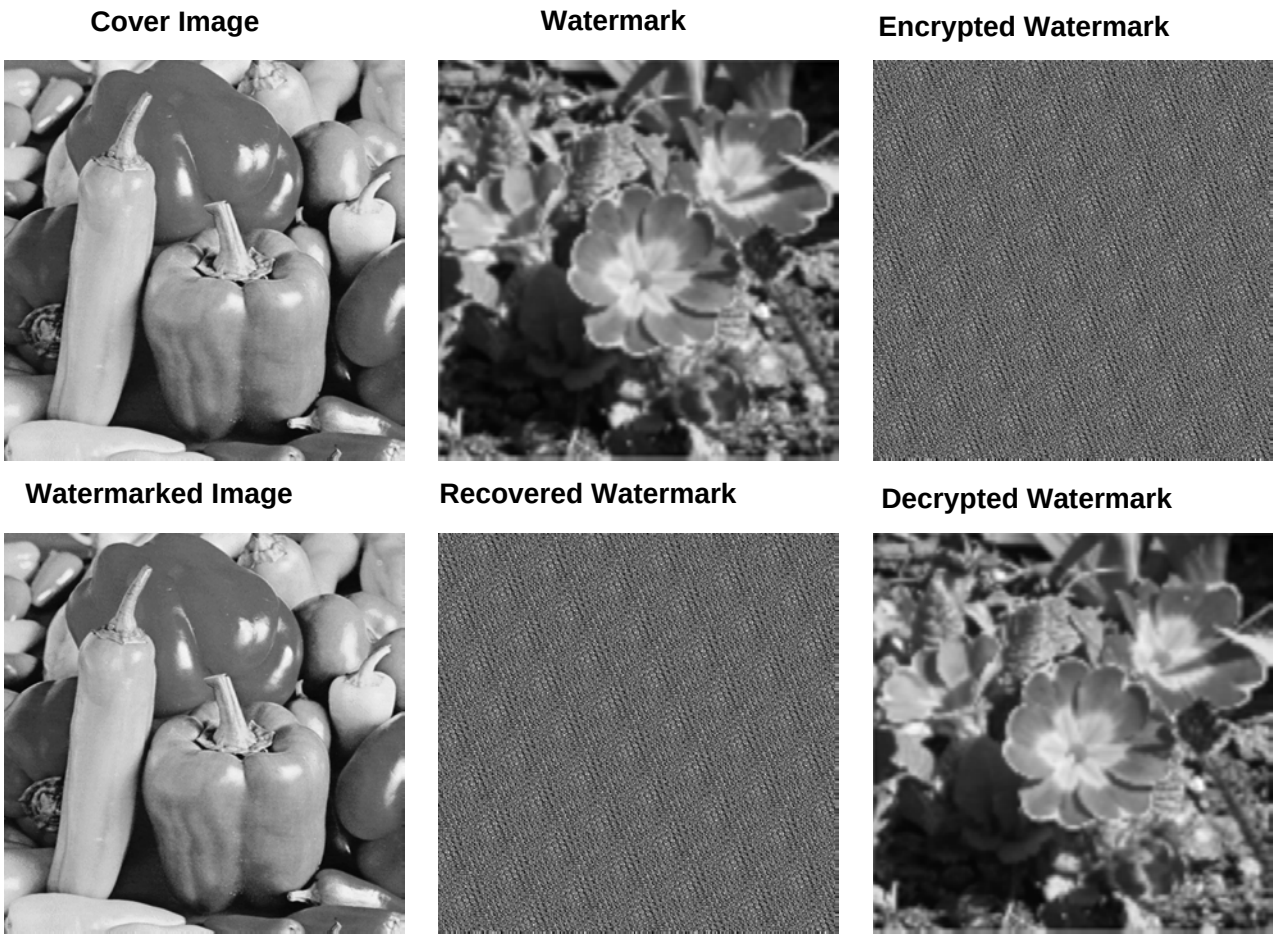

Fig.4.1 Experimental Results of Peppers Cover Image with Flower Watermark.

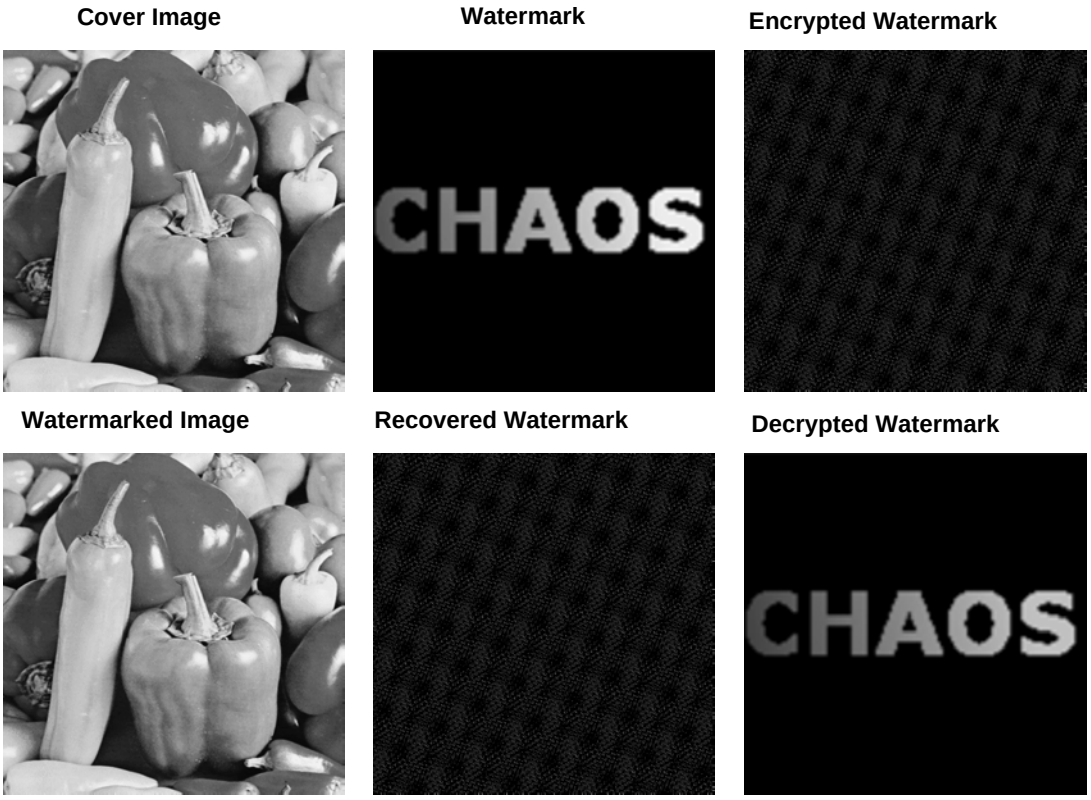

Fig.4.2 Experimental Results of Peppers Cover Image with Chaos Watermark.

In figure Fig. 4.3 Lena Cover image at top left is the original image and Flower image as a watermark in to middle image in figure and encrypted watermark at top right. The bottom right image in figure shows the decrypted watermark and the bottom middle image shows the recovered watermark and bottom right shows the watermarked image. These overflowed chaotic attractor lost the ability of encryption. Therefore the resulted image still maintains the feature of the original image, as shown in figure

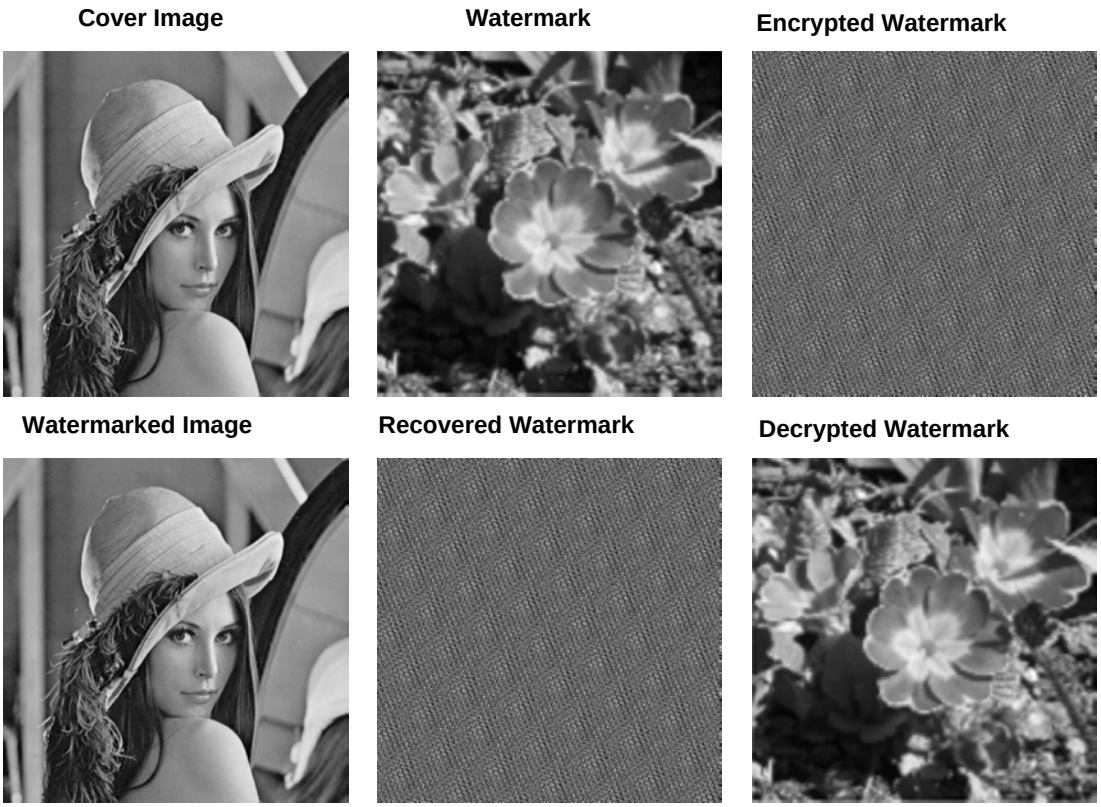

Fig.4.3 Experimental Results of Lena Cover Image with Flower Watermark.

In figure Fig. 4.4 Lena Cover image at top left is the original image and CHAOS image as a watermark in to middle image in figure and encrypted watermark at top right. The bottom right image in figure shows the decrypted watermark and the bottom middle image shows the recovered watermark and bottom right shows the watermarked image. These overflowed chaotic attractor lost the ability of encryption. Therefore the resulted image still maintains the feature of the original image, as shown in figure

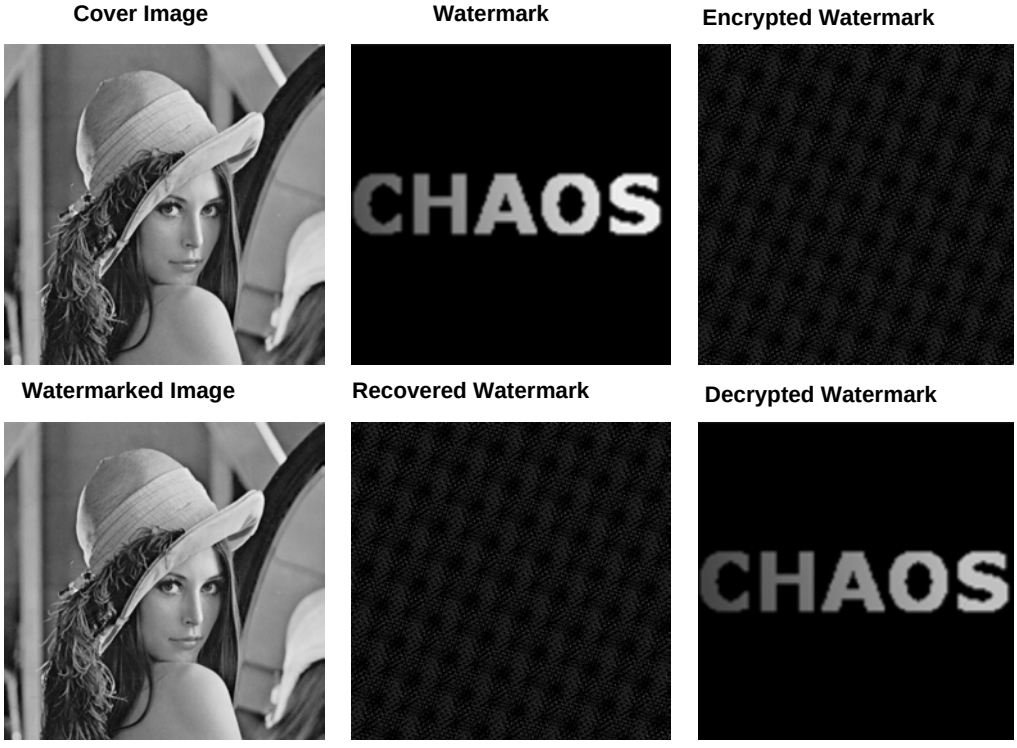

Fig. 4.4 Experimental Results of Lena Cover Image with Chaos Watermark.

The same simulation analysis of proposed algorithm has been performed for Baboon Cover Image with Flower Watermark and Baboon Cover Image with Chaos Watermark as shown in Fig. 4.5 and Fig. 4.6 respectively.

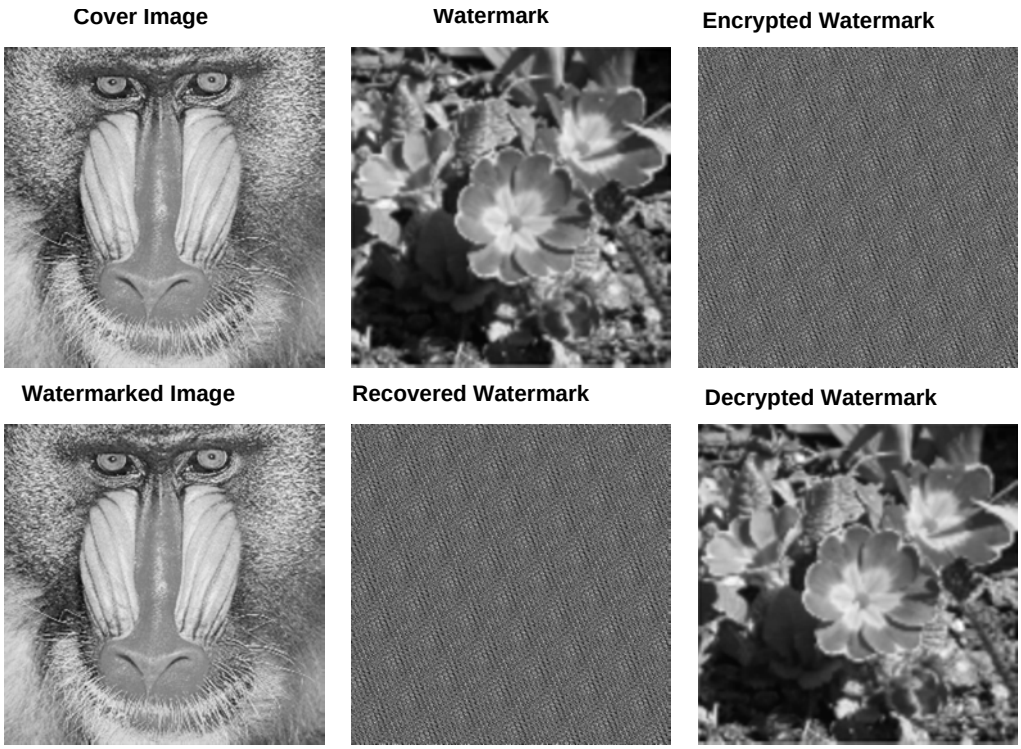

Fig.4.5 Experimental Results of Baboon Cover Image with Flower Watermark.

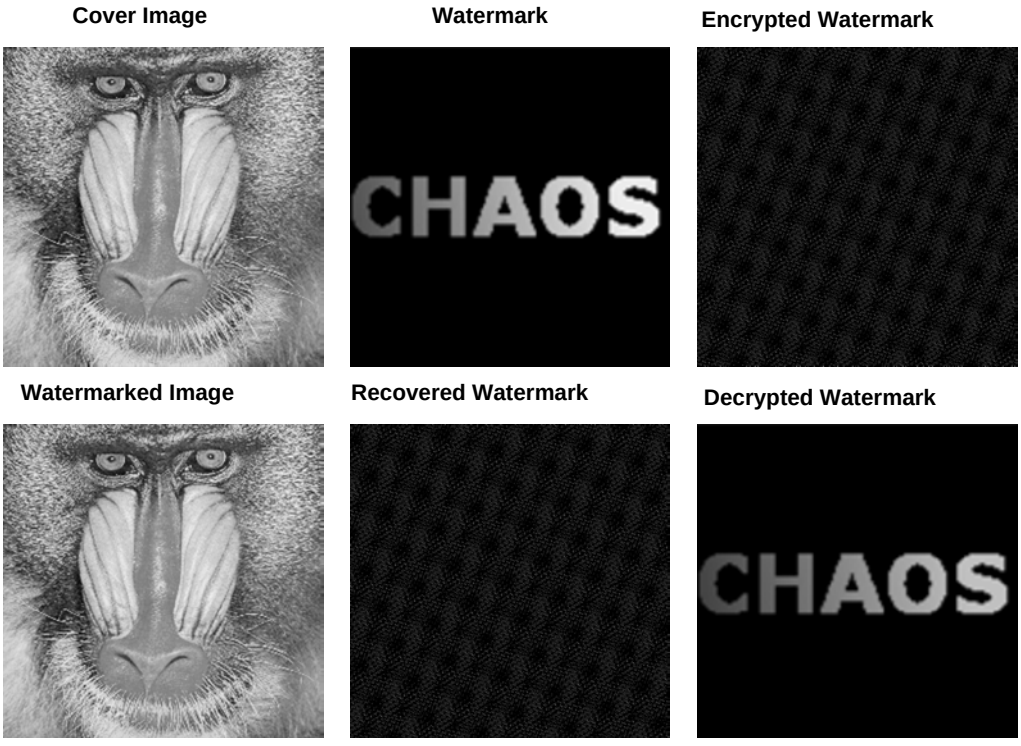

Fig.4.6 Experimental Results of Baboon Cover Image with Chaos Watermark.

The performance comparison of proposed work with existing work in terms of PSNR and SSIM has shown in Table 1 and Table 2 respectively it can be concluded that proposed work has better performance as compare to previous work against security and robustness.

Fig. 4.7 and Fig. 4.8 shows the graphical representation of PSNR and SSIM comparison of proposed and previous work.

Table 1: Performance Comparison of PSNR

Cover Image/ Secret Data	***Lena***		***Baboon***		***Peppers***	
Method	***Previous[1]***	***Proposed(Our)***	***Previous[1]***	***Proposed(Our)***	***Previous[1]***	***Proposed(Our)***
Chaos	51.1743	104.37 dB	51.1726	104.37 dB	51.1912	104.37 dB
Flower	51.1768	95.79 dB	51.1712	95.79 dB	51.1682	95.79 dB

Table 2: Performance Comparison of SSIM

Cover Image/ Secret Data	***Lena***		***Baboon***		***Peppers***	
Method	***Previous[1]***	***Proposed(Our)***	***Previous[1]***	***Proposed(Our)***	***Previous[1]***	***Proposed(Our)***
Chaos	0.9962	1.0000	0.9987	1.0000	0.9963	1.0000
Flower	0.9962	0.9999	0.9987	0.9999	0.9963	0.9999

.

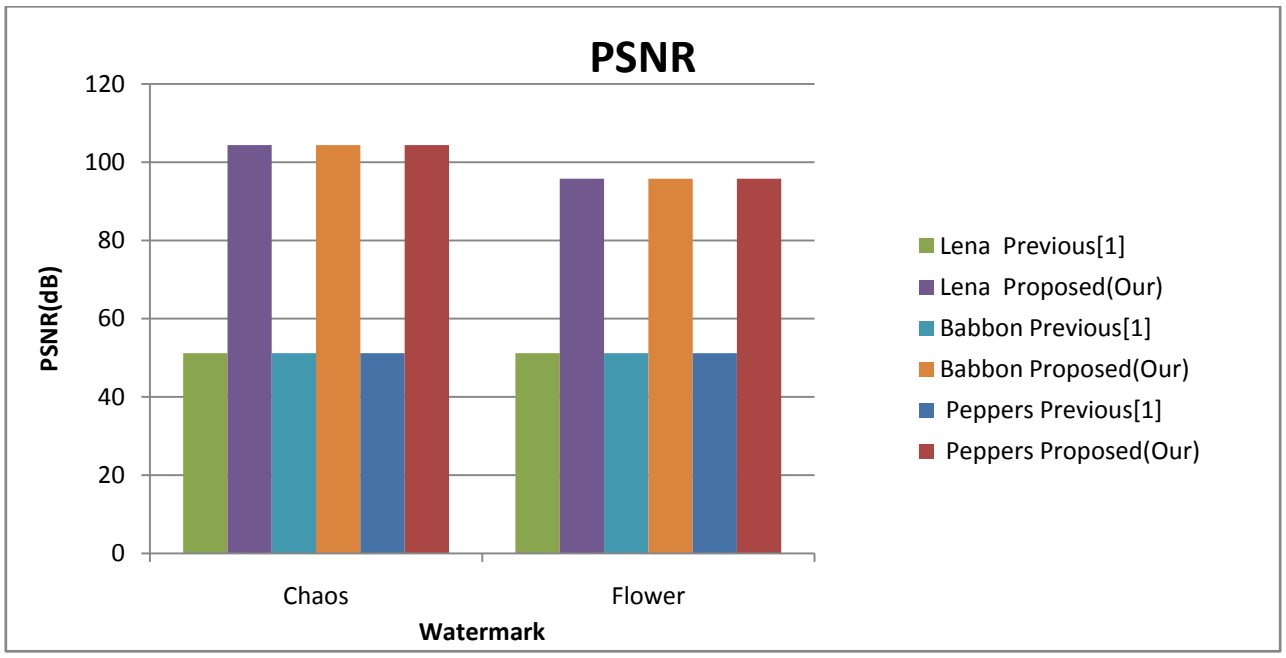

Fig.4.7 Graphical Comparison of PSNR for All Images.

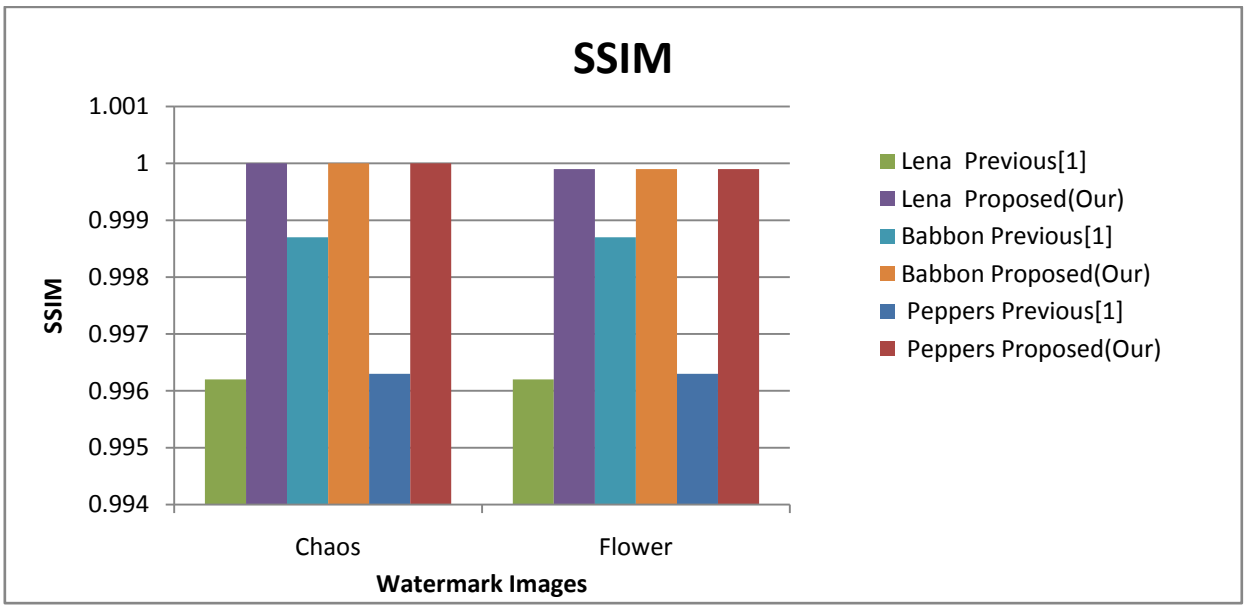

Fig.4.8 Graphical Comparison of SSIM for All Images.

V. CONCLUSION AND FUTURE SCOPE

This examination brief a secured 3-level Wavelet Decomposition Steganography using Arnold Chaotic Map algorithm based, the simulation experiments show that this algorithm is capable of achieving good effects in encryption and decryption. It is shown from the algorithm security analysis that it has large key space, strong sensitivity of encryption key and good statistical characteristics. From the simulation and results analysis the comparison between previous and proposed work has made. The proposed work shows the better PSNR and SSIM as compared to previous work. Based on PSNR and SSIM comparison and can be said that proposed is better than previous one. Therefore, the future research shall focus on the theoretical deduction of improvement method of chaotic sequence and optimization of encryption algorithm, so that it can achieve better encryption/decryption effects and resist diversified attacks.

REFERENCES

[1]. J. Oravec and J. Turán, "Substitution steganography with security improved by chaotic image encryption," 2017 IEEE 14th International Scientific Conference on Informatics, Poprad, 2017, pp. 284-288.

[2]. P. Praveenkumar, R. S. Devi, K. Thenmozhi, J. B. B. Rayappan and R. Amirtharajan, "Stego integrated image encryption using row and column indexing — An information security," 2017 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, 2017, pp. 1-4.

[3]. J. Miao, Y. Xiao, Z. Su and Y. Liang, "A Steganography System Based on Dual Chaotic Encryption and Singular Value Shifting," 2016 6th International Conference on Digital Home (ICDH), Guangzhou, 2016, pp. 6-10.

[4]. P. Tamilselvi and M. Manikandan, "Prediction error and histogram shifting based reversible data hiding," 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), Chennai, 2015, pp. 1-5.

[5]. A. K. Mohan, M. R. Saranya and K. Anusudha, "Improved reversible data hiding using histogram shifting method," 2015 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), Kozhikode, 2015, pp. 1-5.

[6]. A. K. Mohan, M. R. Saranya and K. Anusudha, "An algorithm for enhanced image security with reversible data hiding," 2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore, 2014, pp. 1042-1045.

[7]. Q. Zhang, "Study on Image Encryption Algorithm Based on Chaotic Theory," 2013 International Conference on Information Science and Cloud Computing Companion, Guangzhou, 2013, pp. 635-639.

[8]. V. Ba´noci, G. Buga´r, D. Levicky´, Z. Klenovicˇova´, ”A Novel JPEG Stega- nography Method Based on Modulus Function with Histogram Analysis,” Radioengineering, 2012, vol. 21, no. 2, p. 758–763. ISSN: 1805-9600.

[9]. J. K. Saini, H. K. Verma, ”A Hybrid Approach for Image Security by Combining Encryption and Steganography”, Proc. of 2nd Intl. Conf. ICIIP 2013, Waknaghat (India), 2013, p. 607–611. ISBN: 978-14-6736- 101-9. DOI: 10.1109/ICIIP.2013.6707665.

[10]. R. Matthews, ”On the Derivation of a ’Chaotic’ Encryption Algo- rithm,” Cryptologia, 1989, vol. 8, no. 6 p. 29–41. ISSN: 0161–1194. DOI: 10.1080/0161-118991863745.

[11]. J. Fridrich, ”Symmetric Ciphers Based on Two-dimensional Chaotic Maps,” Intl. J. of Bifurcation and Chaos, 1998, vol. 8, no. 6, p. 1259– 1284. ISSN: 0218–1274. DOI: 10.1142/S021812749800098X.

[12]. F. J. S. Moreira, ”Chaotic dynamics of quadratic maps,” Master’s thesis, University of Porto (Portugal), 1992, 50 p.