International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

Chaotic Encryption Approach For Image With Enhanced Security Features By Added Watermarking Scheme

Arjumand Rizvi, Gopi Kishan Yadav
Computer Science and Engineering,
Bansal Institute Of Engineering And Technology, Lucknow
arizvi0512@gmail.com, gopi.yadav2010@gmail.com

Abstract: In this paper, we focus on the subject of joint image compression and encryption. Presently the internet multimedia applications have become very popular. Valuable multimedia content like digital images and videos are vulnerable to unauthorized access while in storage and during transmission over a wireless network. Streaming of the digital images has requirement of high network bandwidth quality for transmission over long distance. For effective image transmission over Internet both security and bandwidth issues must be considered. In this work, we present a novel scheme, which combines Discrete Wavelet Transform (DWT) for image and block cipher with chaotic encryption for image with watermarking add on. The simulation results indicate that our proposed method enhances the security for image transmission over the Internet as well as improves the recovery rate.

Keywords: Decryption, Encryption, Image encryption, Symmetric key cryptography.

1. Introduction:

There are few approaches designed for protecting data and securing systems. One of them is data encryption (cryptography). Only a person who possesses appropriate key (or keys) can decrypt the encrypted data. The drawback of this data protection strategy is that once such a data is decrypted by a pirate, there is no way to protect the data and track the illegal distribution. Also it is impossible legally to prove the ownership. The next approach to protect the intellectual property rights is watermarking. Watermarking is a technique for embedding hidden data that attaches copyright protection information to digital information.This provides an indication of ownership of the digital data.

Watermarking is closely related to steganography in that they are both concerned with covert communication and belong to a broader subject known as information hiding. Steganography, derived from Greek, literally means "covered writing" is the art of hiding information inside other data in ways that prevent the detection of hidden message. A steganographic system is typically not required to be robust against intentional removal of the hidden message. On the other hand, the watermarking requires that the hidden message should be robust to attempts aimed at removing it. In the case of copyright protection the copyright information should resist any modifications by pirates intending to remove it. This is a significant step forward compared to a common steganography.

Watermarking is either "*visible*" or "*invisible*". Perceptible mark ("*visible watermark*") of ownership or authenticity has been around for centuries in the form of stamps, seals, signatures or classical watermarks. Nevertheless, for known data manipulation technologies the imperceptible digital watermarks are mandatory in most of applications. The up to date known watermarking applications considered in the open literature are as follows [2]:

- *Copyright Protection:* for the protection of the intellectual property, the data owner can embed a watermark representing copyright information in the data. The embedded watermark can be used as a proof, e.g. in a court if someone intentionally infringed the copyrights.
- *Fingerprinting:* to trace the source of illegal copies, the owner can use the fingerprinting technique. In this case, the owner can embed different watermarks in the copies of the data that are supplied to different customers. Fingerprinting can be compared to embedding a serial number that is related to the customer's identity in the data. It enables the intellectual property owner to identify customers who have broken their license agreement by supplying the data to third parties.
- *Copy protection:* the information stored in watermark can directly control digital recording devices for copy protection purposes. In this case the watermark represents a copy-prohibit bit and watermark detectors in the recorder determine whether the data offered to the recorder may be stored or not.

• *Broadcast monitoring:* by embedding a watermark in commercial advertisements, an automated monitoring system can verify whether the advertisements are broadcasted as contracted. Broadcast monitoring can protect not only the commercials but also the valuable TV products.
• *Data authentication:* the so called fragile watermarks can be used to check the authenticity of data. A fragile watermark indicates whether the data has been altered. Further it offers the information in which part the data are being altered.
• *Indexing:* indexing of video mail, where comments can be embedded in the video content; indexing of movies and news items, where markers and comments can be inserted in order to be used by search engines.
• *Medical safety:* embedding the date and the patient's name in medical images could be a useful safety measure.
• *Data Hiding:* watermark techniques can be used for the transmission of secret messages. Since various governments restrict the use of encryption services, people can hide their messages in other data.

2. Related Work:

In **2010, Jamal A. Hussein** proposed there work related to spatial domain watermarking scheme for colored images based on log-average luminance. In this work ,a new watermarking scheme was presented based on log-average luminance. A colored-image was divided into blocks after converting the RGB colored image to ycbcr color space. A monochrome image of 1024 bytes was used as the watermark. To embed the watermark, 16 blocks of size 8X8 are selected and used to embed the watermark image into the original image. The selected blocks were chosen spirally (beginning form the centre of the image) among the blocks that have log-average luminance higher than or equal the log-average luminance of the entire image. Each byte of the monochrome watermark was added by updating a luminance value of a pixel of the image. If the byte of the watermark image represented white color (255) a value α is added to the image pixel luminance value, if it is black (0) the α is subtracted from the luminance value. To extract the watermark, the selected blocks are chosen as the above, if the difference between the luminance value of the watermarked image pixel and the original image pixel is greater than 0, the watermark pixel was supposed to be white, otherwise it supposed to be black. Experimental results showed that the proposed scheme was efficient against changing the watermarked image to grayscale, image cropping, and JPEG compression.

In 2011, Manjit Thapa et. Al presented there work related to secure digital image watermarking techniques. In this work, they stated that digital watermarking was used to hide the information inside a signal, which can not be easily extracted by the third party. Its widely used application was copyright protection of digital information. It was different from the encryption in the sense that it allowed the user to access, view and interpret the signal but protect the owner-ship of the content. One of the current research areas was to protect digital watermark inside the information so that ownership of the information cannot be claimed by third party. With a lot of information available on various search engines, to protect the ownership of information is was a crucial area of research. In latest years, several digital watermarking techniques were presented based on discrete cosine transform (DCT), discrete wavelets transform (DWT) and discrete fourier transforms (DFT). In this work, we proposed an algorithm for digital image watermarking technique based on singular value decomposition; both of the L and U components are explored for watermarking algorithm. This technique refered to the watermark embedding algorithm and watermark extracting algorithm. The experimental results proved that the quality of the watermarked image was excellent and there was strong resistant against many geometrical attacks.

In 2012, Kaushik Deb proposed there work related to combined dwt-dct based digital image watermarking technique for copyright protection .There work stated a combined DWT and DCT based watermarking technique with low frequency watermarking with weighted correction is proposed. DWT has excellent spatial localization, frequency spread and multi-resolution characteristics, which were similar to the theoretical models of the human visual system (HVS). DCT based watermarking techniques offer compression while DWT based watermarking techniques offer scalability. These desirable properties were used in this combined watermarking technique. In the proposed method watermark bits were embedded in the low frequency band of each DCT block of selected DWT sub-band. The weighted correction was also used to improve the imperceptibility. The extracting procedure reversed the embedding operations without the reference of the original image. Compared with the similar approach by DCT based approach and DWT based approach, the experimental results showed that the proposed algorithm apparently preserved superior image quality and robustness under various attacks such as JPEG compression, cropping, sharping, contrast adjustments and so on.

In 2012, Yusuf Perwej et. Al. Proposed there work related to an adaptive watermarking technique for the copyright of digital images and digital image protection .In this work they stated that internet as a whole does not use secure links, thus information in transit may be vulnerable to interruption as well. The important of reducing a chance of the information being detected during the transmission is being an issue in the real world now days. The Digital watermarking method provides for the quick and inexpensive distribution of digital information over the Internet. This method provides new ways of ensuring the sufficient protection of copyright holders in the intellectual property dispersion process. The property of digital watermarking images allows insertion of additional data in the image without altering the value of the image. This message is hidden in unused visual space in the image and stays below the human visible threshold for the image. Both seek to embed information inside a cover message with little or no degradation of the cover-object. In this work investigate the following relevant concepts and terminology, history of watermarks and the properties of a watermarking system as well as a type of watermarking and applications. We are proposing edge detection using Gabor Filters. In this work they proposed least significant bit (LSB) substitution method to encrypt the message in the watermark image file. The benefits of the LSB are its simplicity to embed the bits of the message directly into the LSB plane of cover-image and many techniques using these methods. The LSB does not result in a human perceptible difference because the amplitude of the change is little therefore the human eye the resulting stego image will look identical to the cover image and this allows high perceptual transparency of the LSB. The spatial domain technique LSB substitution it would be able to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given key. They were using DCT transform watermark algorithms based on robustness. The watermarking robustness have been calculated by the Peak Signal to Noise Ratio (PSNR) and Normalized cross correlation (NC) is used to quantify by the Similarity between the real watermark and after extracting watermark.

In 2013 Bhupendra Ram et. Al. (IEEE) proposed there work related to digital image watermarking technique using discrete wavelet transform and discrete cosine transform. In this work they stated that digital watermarking has been proposed as a viable solution to the need of copyright protection and authentication of multimedia data in a networked environment, since it makes possible to identify the author, owner, distributor or authorized consumer of a document. In this work a new watermarking technique to add a code to digital images is presented: the method operates in the frequency domain embedding a pseudo-random sequence of real numbers in a selected set of DCT coefficient and a new method for digital image watermarking which does not require the original image for watermark detection. The watermark is added in select coefficients with significant image energy in the transform domain in order to ensure non- erasability of the watermark. Advantages of the proposed method include: improved resistance to attacks on the watermark, implicit visual masking utilizing the time-frequency localization property of wavelet transform and a robust definition for the threshold which validates the watermark.. Experimental results demonstrated that this proposed technique was robust to most of the signal processing techniques and geometric distortions.

3. Genetic Algorithm:

The genetic algorithm is optimization and search technique based on the principles of genetics and natural selection.

GA composed of five components that are random number generator, fitness evaluation unit and genetic operators for reproduction, crossover and mutation operations. The initial population required at the start of the algorithm is a set of number strings generated by the random number generator. Each string is a representation of a solution to the optimization problem being addressed. Associated with each string is a fitness value (fval) computed by the evaluation unit. The reproduction operator performs a natural selection function known as “seeded selection”. Individual strings are copied from one set to the next according to the fitness values, the higher the fitness value, the greater is the probability of a string being selected for the next generation. The crossover operator chooses pairs of strings at random and produces new pairs. The mutation operator randomly mutates or reverses the values of bits in a string. A phase of algorithm consists of applying the evaluation, reproduction, crossover and mutation operations. A new generation of solutions is produced with each phase of the algorithm.

4. The Concepts of Image Encryption

Image encryption is necessary for future multimedia Internet applications. Password codes to identify individual users will likely be replaced are biometric images of fingerprints and retinal scans in the future. However, such information will likely be sent over a network. When such images are sent over a network, an eavesdropper may duplicate or reroute the

information. By encrypting these images, a degree of security can be achieved. Furthermore, by encrypting noncritical images as well, an eavesdropper is less likely to be able to distinguish between important and non-important information.

Image encryption can also be used to protect privacy. An example for image encryption to protect privacy is in medical imaging applications. Recently, in order to reduce the cost and to improve service, electronic forms of medical records have been sent over networks from laboratories to medical centers.

According to the law, medical records, which include many images, should not be disclosed to any unauthorized persons. Medical images, therefore, should be encrypted before they are sent over networks.

Unlike the conventional cryptographic algorithms, which are mainly based on discrete mathematics, chaos-based cryptography is relied on the complex dynamics of nonlinear systems or maps, which are deterministic but simple. Chaotic maps present many desired cryptographic qualities such as simplicity of implementation that leads
to high encryption rates, and excellent security. Therefore, it can provide a fast and secure means for data protection, which is crucial for image data transmission over fast communication channels, such as the broadband Internet communication [46-49].

The main obstacle in designing image encryption algorithms is that it is rather difficult to swiftly confuse and diffuse data by traditional means of cryptology. In this respect, chaos-based ciphers have shown their superior performance. It has been proved that in many aspects that chaotic maps have analogous but different characteristics as compared with conventional encryption algorithms [12].

The Ciphering of image is actually an important issue. One essential difference between text data and image data is that the size of image data is much larger than the text data. The time is very important factor for the image encryption [1]. Two levels of time are found, the first is the time to encrypt, and the other is the time to transfer images. To minimize it, the first step is to choose a robust and easy method to implement cryptosystem. Two approaches of select encryption where wavelet-based methods are used for compression [2]. The first attempt
was to hide the choice of filters, while the second approach of selective encryption was based on wavelet packets and the decomposition tree is keep secret. The use of genetic algorithm is very important tool to find more secure image, where genetic algorithm gives suitable key stream.

4.1 Features of Image Encryption Schemes

Unlike text messages, image data have their special features such as high redundancy, and high correlation among pixels. Also, they are usually huge in size, which together makes traditional encryption methods difficult to apply and slow to process. Sometimes, image applications have their own requirements like real-time processing, fidelity reservation, image format consistence, and data compression for transmission, etc. Simultaneous fulfillment of these requirements along with high security and high quality demands has presented great challenges to real-time imaging
practice. For studying image encryption, we must first analyze the differences between implementations for image data and text data. Basically, there are some differences between image and text as follows [6]:

1. When the ciphertext is produced, it must be decrypted to the original plaintext in a full lossless manner. However, the cipherimage can be decrypted to the original plainimage in some lossy manner.
2. Text data are sequences of words. It can be encrypted directly by using block or stream ciphers. However, digital images are usually represented as 2D arrays. For protecting the stored 2D data, they must be converted to 1D arrays
before using various traditional encryption techniques.
3. Since the storage space of a picture is very large, it is inefficient to encrypt or decrypt images, directly. One of the best methods is to only encrypt/decrypt information that is used by image compression for reducing both its storage
space and transmission time.

5. The Encryption Evaluation Metrics

In this section, we will discuss, in detail, two families of encryption metrics; the first family evaluates the ability of the encryption algorithm to substitute the original image with uncorrelated encrypted image. In This family, five metrics, which are the histogram deviation DH, the correlation coefficient rxy, the irregular deviation DI, the
histogram uniformity, and a proposed encryption quality metric, are studied. The second family evaluates the diffusion characteristics of the encryption algorithm. In this family, three metrics, which are the Avalanche effect, NPCR and UACI, are studied.

5.1 The Histogram Deviation

The histogram deviation measures the quality of encryption in terms of how it maximizes the deviation between the original and the encrypted images [79]. The steps of calculating this metric are:

1. Estimate the histogram of both the original and the encrypted images.
2. Estimate the absolute difference between both histograms.

3. Estimate the area under the absolute difference curve, divided by the total area of the image, as follows:

$$D_H = \frac{(\frac{d_0+d_{255}}{2}+\sum_{i=1}^{254} d_i)}{MxN} \quad 1$$

where di is the amplitude of the absolute difference curve at the gray level i. M and N are the dimensions of the image to be encrypted. The higher the value of DH is, the better the quality of the encrypted image [79].

Although this measure of quality will give good results about how the encrypted image is deviated from the original image, it can't be used alone to measure the quality of encryption as it has some limitations as will explained later.

5.2 The Correlation Coefficient

A useful measure to assess the encryption quality of any image cryptosystem is the correlation coefficient between pixels at the same indices in the plain and the cipher images [79]. This metric can be calculated as follows:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad 2$$

where x and y are the gray-scale values of two pixels at the same indices in the plain and cipherimages. In numerical computations, the following discrete formulas can be used:

$$E(x) = \frac{1}{L}\sum_{l=1}^{L} x_l \quad 3$$

$$D(x) = \frac{1}{L}\sum_{l=1}^{L}(x_l - E(x))^2, \quad 4$$

$$COV(x, y) = \frac{1}{L}\sum_{l=1}^{L}(x_l - E(x))(y_l - E(y)), \quad 5$$

where L is the number of pixels involved in the calculations. The closer the value of *xy r* to zero is, the better the quality of the encryption algorithm.

5.3 The Irregular Deviation

The irregular deviation measures the quality of encryption in terms of how much the deviation caused by encryption (on the encrypted image) is irregular [10].

The steps of calculating this metric are:

1. Calculate the absolute difference between the encrypted image and the original image.
2. Estimate the histogram H of this absolute difference matrix.
3. Estimate the mean value MH of this histogram.
4. Estimate the absolute of the histogram deviations from this mean value as follows:

$H_D(i) = |H(i) - M_H|$

The irregular deviation DI is calculated as follows:

$$D_I = \frac{\sum_{i=0}^{255} H_D(i)}{MxN} \quad 6$$

The lower the value of *DI* is, the better the encryption quality.

5.4 The Histogram Uniformity

A histogram uses a bar graph to profile the occurrence of each gray level of the image. The horizontal axis represents the gray-level value. It begins at zero and goes to the number of gray levels Each vertical bar represents the number of times of corresponding gray level occurred in the image [11].

For image encryption algorithms, the histogram of the encrypted image should have two properties

1. It must be totally different of the histogram of the original image.
2. It must have a uniform distribution, which means that the probability of existence of any gray scale value is the same, and it is totally random. This test was made using the MATLAB built in function (imhist).

5.5 Noise Immunity

The noise immunity reflects the ability of the image cryptosystem to tolerate noise. To test the noise immunity, noise with different signal to noise ratios (SNRs) is added to the encrypted image, and then the decryption algorithm is performed. If the decrypted image is close to the original image, we can say that the cryptosystem at hand is immune to noise. This closeness can be verified visually or numerically with the value of *xyd r* , which represents the correlation coefficient between the original image and the decrypted image, and the peak signal to noise ratio (PSNR) of the decrypted image, which is defined as follows [79, 85] :

$$PSNR = 10x\log_{10}\left(\frac{MxNx255^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}|(f(m,n)-f_d(m,n))|^2}\right) \quad 7$$

where *f m, n* is the original image and , *d f m n* is the decrypted image.

5.6 The Processing Time

The processing time is the time required to encrypt and decrypt an image. The smaller the processing time is, the better the encryption efficiency.

6. Result and Discussion:

The proposed algorithms are tested and evaluated on the digital image database using MATLAB. In this work a watermark image is encrypted using chaotic unction and genetic algorithm. After that the encrypted watermark image is embedded into the original image. Finally the watermarked image is produced and shown. The Watermarking parameters can be tested

after extracting the original image from the water marked image. It can be observed that the proposed approach preserves the high perceptual quality of the watermarked image.

As a measure of the quality of a watermarked image, the peak signal-to noise ratio (PSNR) is used. To evaluate the robustness of the proposed approach, the watermarked image is tested against different kinds of attacks. For comparing the similarities between the original and extracted watermarks, the Pearson's correlation coefficient was employed. After studying the experimental results, it can be seen that the proposed scheme significantly outperforms the two compared schemes. In addition to quantitative measurement, we also need the visual perceptions of the extracted watermarks. The constructed watermarks with best-quality measurement are shown and we can find that our scheme not only can successfully resist different kinds of attacks but can also restore watermark with high perceptual quality.

In order to test the proposed approach of watermarking algorithm, a watermark embedding is made of a "Lena" image of 256*256.The watermarking is a "pout" image. The results are shown in figure 1

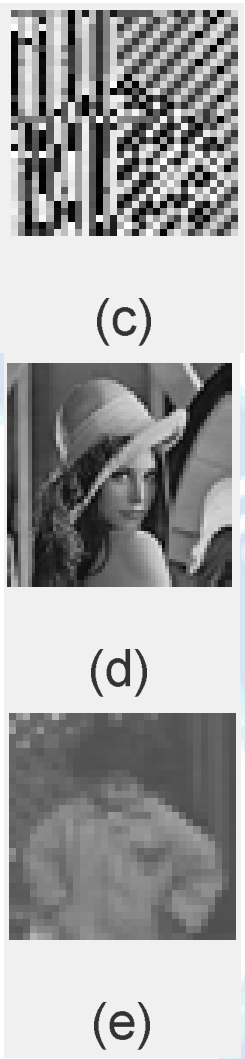

Fig 1: (a) is original image, (b) original watermark image, (c) watermark image after chaos with optimized GA encryption, (d) is the watermark embedded image and (e) is the watermark image after extraction and decryption process.

As a test of the embedding, Peak noise to signal rations (PSNR) and similarity degree are chosen as detection indexes. From the figures, we can see that (d) keeps a good quality with a PSNR=85.16dB.Where PSNR is higher than 30dB; it is hard to distinguish between original image and the reconstructed one. Figure (e) is also highly similar to original watermarking (NC=1.0).There is nearly no visible difference. So this algorithm is of good invisibility.

A good encryption algorithm is one in which the correlation coefficients between pairs of encrypted adjacent pixels are at the least possible level. In Figure(c) correlation coefficient is -0.2419 hence this algorithm also provides higher security.

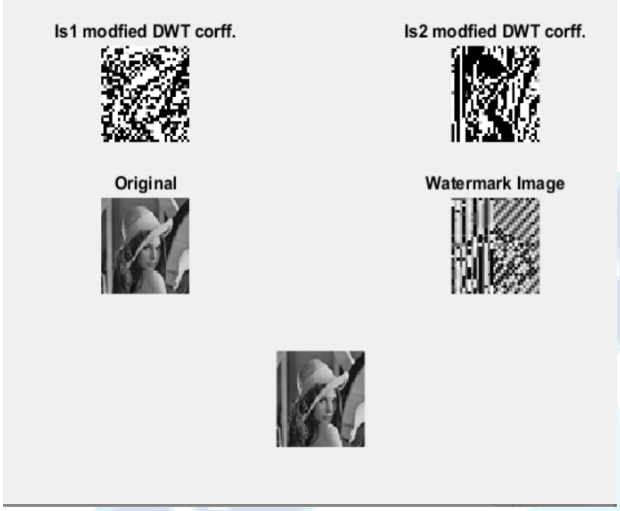

Fig 2: Modified DWT coefficient after encryption (top) ,Original image and image to be watermarked (bottom) water marked image.

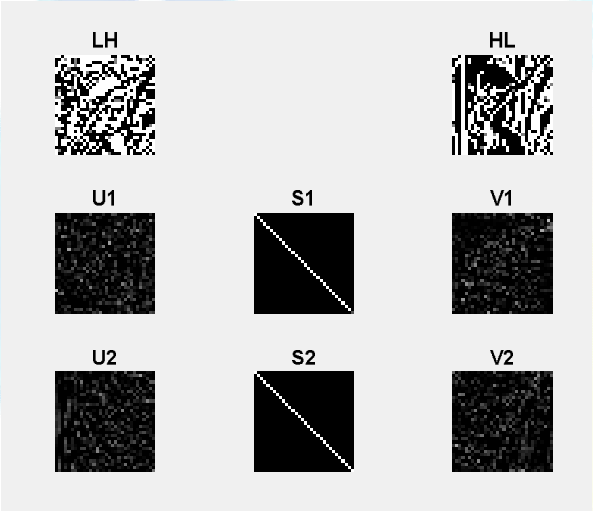

Fig 3: HL and LH wavelet component (top) SUV component of LH and HL (middle and bottom)

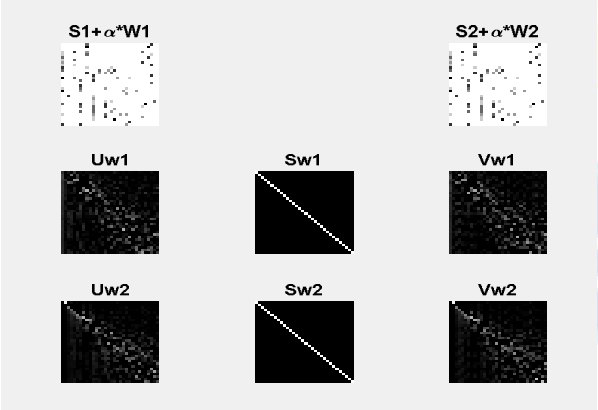

Fig 4: Embedding of watermark W1 and W2 with S1 and S2 (top), modified USV component after embedding watermark image (middle and bottom).

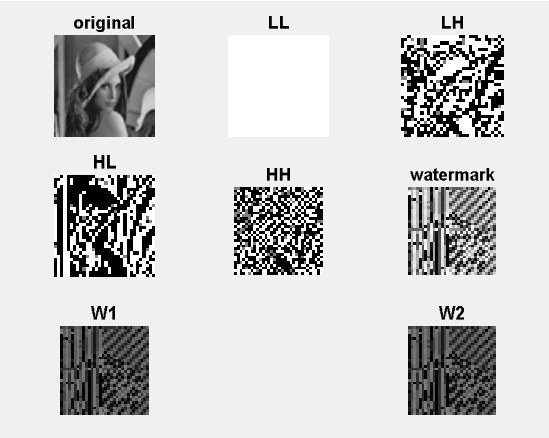

Fig 5:Orignal image and its LL,LH DWT component (top).HL,LH DWT component of original image and encrypted watermark image(middle).W1 and W2 partition of watermark image.(bottom)

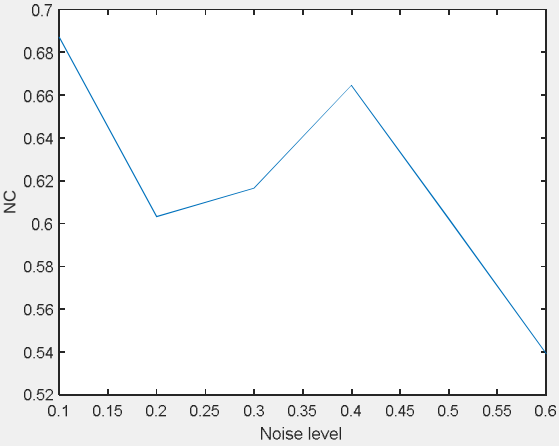

Fig 6: Normalization coefficient with respect to different nosie level.

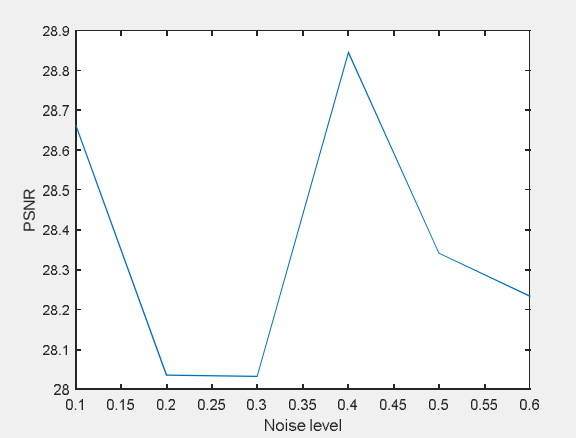

Fig 7: PSNR value with respect to different nosie level.

5. Conclusion:

In this work we have presented a joint image-watermarking technique based on DWT and SVD along with encrypting watermark image by using the chaotic function logistic map and genetic algorithms. Here the watermark is embedded on the singular values of the cover image's DWT sub bands. The technique fully exploits the respective feature of these two transform domain methods: spatial-frequency localization of DWT and SVD efficiently represents intrinsic algebraic properties of an image. Main innovation in this paper is that this is the first time genetic algorithms are used in this way to encrypt watermark image. The idea of embedding encrypted watermark image into original image is to provide more protection in image. Experimental results of the proposed technique have shown both the significant improvement in imperceptibility and the robustness under attacks. In this work, an algorithm based on DWT-SVD and GA based chaos image encryption is referred. The security is enhanced by randomized nature of genetic algorithm and it also provides good robustness.

References:

[1] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryption algorithm and its VLSI architecture", Pattern Recognition and Image Analysis, vol.IO, no.2, pp.236-247, 2000.

[2] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203),229-234.

[3] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001),1229- 1245.

[4] William stallings, ―Cryptography and Network Security: Principles & Practices‖, second edition.

[5] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, ―A Modified AES Based Algorithm for Image Encryption‖, World Academy of Science, Engineering and Technology 27 2007.

[6] Chiou-Ting Hsu1 and Ja-Ling Wu2, "Image Watermarking By Wavelet Decomposition" Academy of Information and Management Sciences Journal, Vol. 3, No. 1, pp. 70-86, 2000

[7] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy "A Dual Digital-Image Watermarking Technique" World Academy of Science, Engineering and Technology 5 2005

[8] Chih-Yang Lin And Yu-Tai Ching "A Robust Image Hiding Method Using Wavelet Technique" JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 22, 163-174 (2006)

[9] Ibrahim Nasir, Ying Weng, Jianmin Jiang " A New Robust Watermarking Scheme for Color Image in Spatial Domain" Signal-Image Technologies and Internet-Based System, 2007. SITIS '07.

[10] Chin-Chen Chang "An Svd Oriented Watermark Embedding Scheme With High Qualities For The Restored Images" International Journal of Innovative Computing, Information and Control ICIC International °c 2007 ISSN 1349-4198 Volume 3, Number 3, June 2007

[11] Ali Al-Haj "Combined DWT-DCT Digital Image Watermarking" Journal of Computer Science 3 (9): 740-746, 2007 ISSN 1549-3636© 2007 Science Publications

[12] B.Chandra Mohan, S. Srinivas Kumar "A Robust Image Watermarking Scheme using Singular Value Decomposition" Journal Of Multimedia, Vol. 3, NO. 1, MAY 2008

[13] Mei Jiansheng, Li Sukang and Tan Xiaomei "A Digital Watermarking Algorithm Based On DCT and DWT" International Symposium on Web Information Systems and Applications (WISA'09)2009.

[14] Tohru Kohda and Akio Tsuneda, "Statistics of chaotic binary sequences," IEEE Trans. Information Technology, vol. 43, no. 1, pp. 104–112, 1997.

[15] Zhou Hong and Ling Xieting, "Generating chaotic secure sequences with desired statistical properties and high security," Int. J. Bifurcation and Chaos, vol. 7, no. 1, pp. 205–213, 1997.

[16] Li Shujun, Mou Xuanqin, and Cai Yuanlong, "Pseudorandom bit generator based on couple chaotic systems and its applications in stream-cipher cryptography," in Progress in Cryptology - INDOCRYPT 2001. 2001, Lecture Notes in Computer Science, vol. 2247, pp. 316–329, Springer-Verlag, Berlin.