International Conference on Intelligent Technologies & Science - 2022
(ICITS-2022)

Chaotic Encryption Approach for Image with Added Watermarking Scheme Enhanced Security Features

Sanjeet Kumar[1], Dakshita Joshi[2]
Computer science and Engineering Department,
Bansal Institute of Engineering and Technology, Lucknow
sanjeet.desire@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.**

Keywords: Image Encryption, Chaos, Chaotic Encryption, Chaotic Image Encryption, Trend Analysis.

1. Introduction:

Digital multimedia data are rapidly spreading everywhere. On the other hand, this situation has brought about the possibility of duplicating and/or manipulating the data. To keep on with the transmission of data over the Internet the reliability and originality of thetransmitted data should be verifiable. It is necessary that multimedia data should beprotected and secured. The design of techniques for preserving the ownership of digital information is in the basic of the development of future multimedia services.

One way to address this problem involves embedding an invisible data into the original data to mark ownership of them. There are many techniques for information hiding, which can be divided into different categories such as convert channels, steganography, anonymity, and watermarking [3]. Convert channels techniques were defined in the context of multilevel secure systems. Convert channels usually handle properties of the communication channels in an unexpected and unforeseen way in order to transfer data

through the medium without detection by anyone other than the entities operating the covert channel. Steganography is about preventing the detection of an encrypted data, which has been protected by cryptography algorithms. Anonymity is a technique to find ways to hide the meta content of tranmitted messages such as sender and the recipients.

Digital watermarking has an extra requirement of robustness compared to steganography algorithms against possible attacks. It should be also noted that watermarking is not intended for protecting of the content of a message, and hence it is different from cryptography. In this thesis we focus on the robustness of the digital watermarking algorithms in the transform domain against common attacks.

2. Related Work:

Another clinical imaging wellbeing and security strategy was presented for Viswanathan P, Venkata Krishna.p [l]. The creator utilized the conventional FED watermarking framework for security purposes. The Fingerprint, Coding and Dual Watermarking System strategy is utilized for getting Teleradiology. The unique finger impression calculation you propose would be utilized to recover the finger impression picture alongside the watermarking of the picture encryption. The fingerprinting calculation offers another strategy for testing and checking the personality of the patient.

In [2] have a cutting edge approach to imparting and sending a picture across the organization. The proposed approach likewise executed a system. A protected organization sharing unique finger impression picture. The reversible secret change is applied to the finger impression picture, alongside halfway straight tumultuous guide. The protected picture is appropriated on the compromised network. The first finger impression picture is reproduced by the converse cycle on the beneficiary hand.

In [3] acquainted a cutting edge arrangement with a tumultuous guide with moving boundaries. The recommended approach has two fundamental highlights: synchronous encoding and message expansion. The technique utilizes a tumultuous deviated tent guide and piece-savvy direct guide to change over broadened messages blocks iteratively into an ASCII code in which boundaries are powerfully altered with the place of the particular message block list and the decimal part is then created which is then flowed to the whole number. The hypothetical assessment and reproduction of the framework's machine uncover a somewhat compelling cycle.

Turbulent casings and wavelet change are important for the proposed stage. The recommended arrangement makes inconsistent groupings by presenting the strategic guide. This alludes to the plaintext being given. The circulated plaintext is then trailed by the change of the wavelet and the problematic issue. The Inverse Wavelet Transform IS was then used to remake the scrambled picture. The calculation testing is

completed based on the key review, which guarantees that a little modification of the key might profit from significant changes, a dim level histogram, hostile to commotion test and hostile to cutting tests. The examination showed that pre-encryption dissemination diminished the strength of the vagueness encryption assault. Because of hazardous cryptography, the aftereffect of dispersion is confidential and the impractical highlights of the document might be unraveled. Another computerized watermarking innovation was created by Lina [5]. The writer utilized in the article to lay out intuitive watermarks the idea of particular wavelet change and turmoil. First the discrete wavelet change is applied to the picture, then the low-recurrence part is taken out, and the wreck succession is applied to scramble the little recurrence component. The principal picture is utilized for extraction, and this is a strategy for non-blind acknowledgment. The NC coefficient and high commotion to flag proportion test the gadget (PNSR). The outcomes proposed that the combination of a consolidated specialized visual culture, a clamor assault, a filtration, and so on. The impact of the watermark picture has been very high [6]. For the information encryption strategy, the creator utilized the calculated arrangement of turmoil. The investigation of the calculation happens on the accompanying standards, like arbitrariness, similarity and intricacy. The turmoil grouping reproduction has shown that it fulfills the standards of the encryption calculation.

3. 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.

3.1 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 [10]. 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:

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

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 [9].

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.

3.2 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 [9]. This metric can be calculated as follows:

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

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:

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

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

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

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.

3.3 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:

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

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

3.4 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).

3.5 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] :

$$\mathrm{PSNR} = 10\mathrm{x}\log_{10}\left(\frac{\mathrm{MxNx}\ 255^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}|(f(m,n)-f_d(m,n))|^2}\right) \qquad 7$$

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

3.6 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.

4. Result and Discussion:

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.

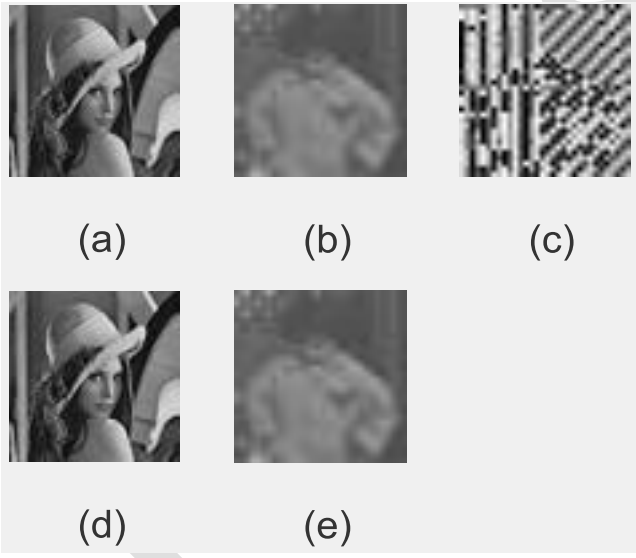

Fig. 1: (a) is original image, (b) original watermark image, (c) watermark image after chaos with optimized GA encryption, (d) is the watermark embedded image and (e) is the watermark image after extraction and decryption process.

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.

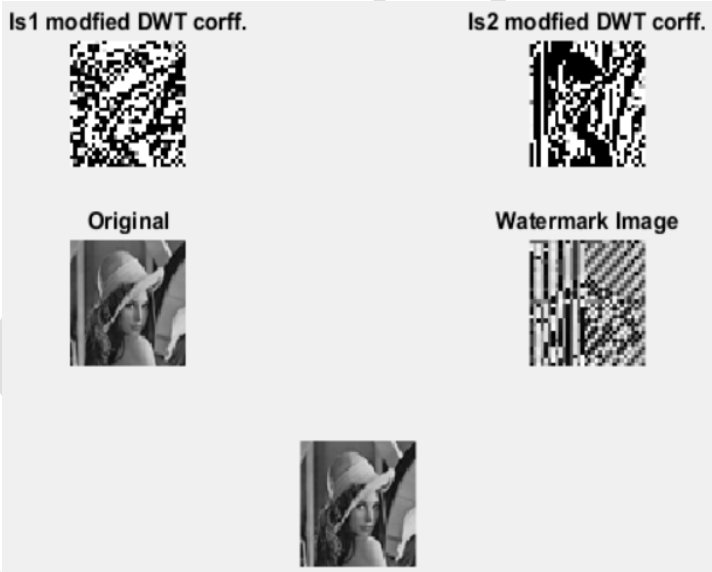

Fig. 2: Modified DWT coefficient after encryption (top) ,Original image and image to be watermarked (bottom) water marked image.

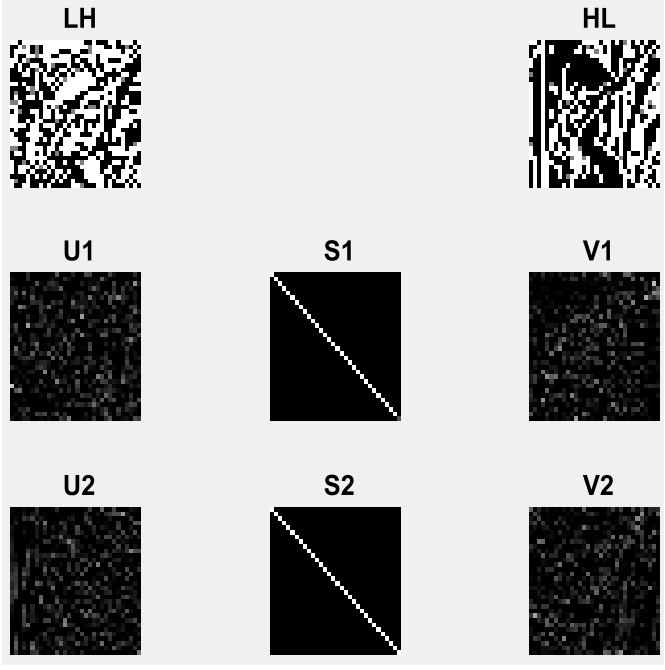

Fig. 3: HL and LH wavelet component (top) SUV component of LH and HL (middle and bottom)

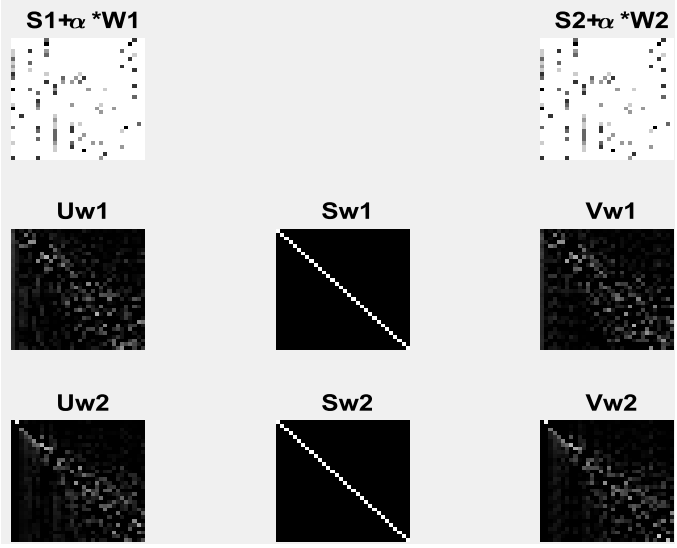

Fig. 4: Embedding of watermark W1 and W2 with S1 and S2 (top), modified USV component after embedding watermark image (middle and bottom).

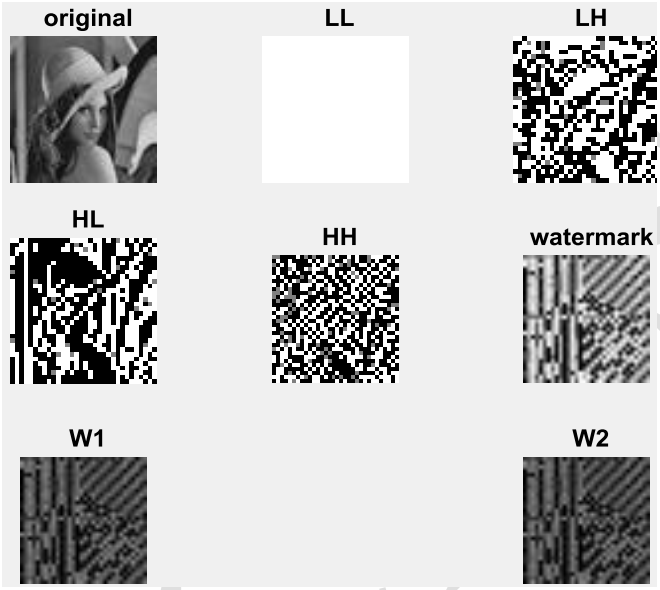

Fig. 5:Orignal image and its LL,LH DWT component (top).HL,LH DWT component of original image and encrypted watermark image(middle).W1 and W2 partition of watermark image.(bottom).

5. Conclusion:

In this work we have presented a joint image-watermarking technique based on DWT and SVD alongwith 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.

References:

[1] P. Viswanathan, Member, P. Venkata Krishna, "A Joint FED Watermarking System using Spatial Fusion for Verifying the Security issues of Teleradiology", IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, pp. 1-12,2013.

[2] Gaurav Bhatnagar and Q. M. Jonathan Wu, "Chaos-Based Security Solution for Fingerprint Data During Communication and Transmission", IEEE TRANSACTIONS ON INSTRUMENT A TION AND MEASUREMENT, VOL. 61, NO.4, pp. 876-887 APRIL 2012.

[3] Yantao Li, Di Xiao, Shaojiang Deng, Qi Han and Gang Zhou, "Parallel Hash function construction based on chaotic maps with changeable parameters", SPRINGER, Neural Computing and Applications, pp. 1305-1312, 17 February 2011.

[4] Runhe Qiu, Y uzhe Fu, Y un Cao, "Image Encryption Research based on chaotic sequences and wavelet stransform", IEEE, pp.1511-1516, 2010.

[5] Qiang Wang, Qun Ding, Zhong Zhang, Lina Ding, "Digital Image Encryption Research Based on DWT and Chaos", IEEE Computer Society Fourth International Conference on Natural Computation, pp. 494-498, 2008.

[6] Gannan Yuan, Research on Data Encryption Technology Based on Chaos Theory", IEEE Computer Society Eighth ACIS International Conference on Sofuvare Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pp. 93-98, 2007.

[7] Guosheng Gu and Guoqiang Han, An Enhanced Chaos Based Image Encryption Algorithm", IEEE Computer Society First International Conference on Innovative Computing, Information and Control, 2006.

[8] Gopal Ghosh et al 2020 IOP Conf. Ser.: Mater. Sci. Eng. 993 012062.

[9] Mazleena Salleh Suhariah Ihrahim Ismail Fauzi lsnin, Enhanced Chaotic Image Encryption Algorithm Based on Baker's Map", IEEE, pp. 508-511, 2003.

[10] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," in IEEE Access, vol. 8, pp. 60539-60551, 2020, doi: 10.1109/ACCESS.2020.2983117.

[11] T. S. Ali and R. Ali, "A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map," in IEEE Access, vol. 8, pp. 71974-71992, 2020.

[12] P. Li and K. -T. Lo, "Survey on JPEG compatible joint image compression and encryption algorithms," in IET Signal Processing, vol. 14, no. 8, pp. 475-488, 10 2020.

[13] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh and G. M. Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption," in IEEE Access, vol. 6, pp. 19876-19897, 2018.

[14] A. Umoh, O. N. Iloanusi and U. A. Nnolim, "Image multi-encryption architecture based on hybrid keystream sequence interspersed with Haar discrete wavelet transform,"

in IET Image Processing, vol. 14, no. 10, pp. 2081-2091, 21 8 2020.
[15] H. Diab, "An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations," in IEEE Access, vol. 6, pp. 42227-42244, 2018.
[16]. Dahiya, M.; Kumar, R. “A literature survey on various image encryption & steganography techniques”. In Proceedings of the First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 15–17 December 2018.
[17]. Makki, Q.H.; Abdalla, A.M.; Tamimi, A.A. A survey of image encryption algorithms. In Proceedings of the International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021.
[18]. Jasra, B.; Moon, A.H. Image encryption techniques: A review. In Proceedings of the 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 29–31 January 2020.