Received: September 6, 2018

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Image Watermarking Using Two Level Encryption Method Based on Chaotic Logistic Mapping and Rivest Shamir Adleman Algorithm

Tipirneni Venugopal[1]* **Vusthikayala Siva Kumar Reddy[2]**

[1]*Rayalaseema University, Kurnool, India*
[2]*MallaReddy College of Engineering and Technology, Hyderabad, India*
* Corresponding author's Email: tipirneni.venu@gmail.com

Abstract: In this research study, a multi-purpose image water-marking approach was developed for delivering self-recovery, ownership verification and tamper localization of the cover image. For robust watermarking, color and grayscale images were used to deliver wide applicability and generalization to proposed work. Initially, the cover image was converted into wavelet domain by using Integer Wavelet Transform (IWT) and then the logo image was encrypted by using chaotic logistic mapping. This procedure makes the digital image free from false positive error and also helps to provide decent capacity. After encryption and transformation, Least Significant Bit (LSB) was used to provide self-recovery feature as well as to locate the tempered region in the digital image. Then, asymmetric encryption algorithm: Rivest–Shamir–Adleman (RSA) was utilized to improve the hidden data security with high computational efficiency, and good embedding capacity. Finally, the experimental outcome shows that the proposed approach delivers a high secure network with low computational complexity by means of entropy value and Peak Signal-to-Noise Ratio (PSNR). The proposed approach improved PSNR value upto 19 dB and entropy value upto 0.07-0.7 compared to the existing methods: Discrete Cosine Transform (DCT) + Arnold transform and differential evolution algorithm.

Keywords: Discrete cosine transform, Integer wavelet transform, Least significant bit, Peak signal-to-noise ratio, Rivest–shamir–adleman, Water-marking.

1. Introduction

In current decades, the rapid growth of multimedia data (video, audio and images) are easily distributed, reprinted and duplicated over internet [1]. So, it is necessary to protect Intellectual Property Right (IPR) of multimedia data. The extensive use of digital and internet data transfer leads to various protection problems pertaining to the ownership of digital resources, especially published digital images [2-4]. In the current scenario, digital watermarking gains more attention as an effective system to protect user's ownership and copyright [5, 6]. In digital watermarking, a (sequence or watermark or trademark) is embedded into the digital images for user's ownership and copyright protection. Usually, the digital grayscale and color images are utilized for digital watermarking either in frequency or spatial domain [7]. In spatial domain, the pixel intensity value of digital images is modified, but watermarking in this domain is not robust. Correspondingly, in frequency domain, the digital image coefficients are modulated by adding extra data and scheme, which becomes more imperceptible.

In frequency domain, several methodologies are used for digital watermarking for gray-scaled and colored digital images in which water-mark log embedded into blue channel as human vision system, which is insensitive to blue channel. In image authentication methods, the visually recognized patterns are embedded as water-mark in low frequency sub-bands, which gives a tradeoff between robustness and imperceptibility. The digital watermarking methodology should contain following three requirements: robust against geometrical, image processing and conventional

attacks, easy extraction with-out affecting the quality of digital images, and transparency or imperceptible. Whereas, developing a computational methodology exhibits these requirements, which is not an easy task. Currently, several watermarking methodologies are developed, where the majority of approaches are based on the transform domain such as, Discrete Wavelet Transform (DWT) [8], Singular Value Decomposition (SVD) [9], Lifting Wavelet Transform (LWT) [10], etc. These methodologies have numbers of inevitable issues such as, poor computational capability and slow learning.

To address this issue, an effective water marking system was developed. In this research paper, RSA algorithm was used to encrypt the digital images for securing the data transmission, but it was relatively slow in encryption process. So, IWT along with chaotic logistic mapping was used in order to accelerate the RSA algorithm to encrypt the image. Compared to the conventional wavelet transforms, IWT along with chaotic logistic mapping decreases the information loss in the extracted logo and cover images. It was the major advantage of proposed methodology, which was not focused in the previous study. For showing the effectiveness of proposed methodology, several images were processed for testing. This research paper is composed as follows. Section 2 surveys several recent watermarking methodologies. In section 3, an effective watermarking strategy is portrayed to seek better security system. In section 4, the execution of proposed technique is assessed by simulation and also comparative analysis is performed between the proposed and existing techniques. The conclusion is done in section 5.

2. Literature review

Several research techniques are proposed by researchers in image watermarking. In this sub-section, brief review of some essential contributions to the existing literatures are presented.

I.A. Ansari, and M. Pant, [11] proposed a multi-purpose image watermarking methodology for providing self-recovery, ownership verification and localization of the host image. In this research, grayscale watermark was used to provide wide applicability and generalization. Initially, the host image was converted into wavelet domain by using DWT and the remaining singular values of converted host were modified on the basis of watermark principal components. At last, the LSB insertion was employed for locating the tempered region and also to provide self-recovery features to the methodology. Additionally, the insertion was optimized by using Artificial Bee Colony (ABC), which helps to maximize the robustness of imperceptibility. The major drawback of developed methodology was stealth (passive or active) affects the presence of message.

H.T. Hu, and L.Y. Hsu, [12] presented a block-based blind watermarking system in the domain of DWT and DCT. Then, Quantization Index Modulation (QIM) was applied to DWT-DCT coefficients for improving the performance of imperceptibility and also to decrease the Bit Error Rate (BER) of extracted watermarks. Additionally, two collective methodologies were proposed to further enhance the efficiency of watermarking. Finally, the experimental outcome confirmed that the proposed methodology has high security compared to the existing methodologies. While employing multi-bit embedding strategy, the time consumption of encryption and decryption system was quite high and also DWT-DCT performed poorly for encrypting the images with homogeneous background.

Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, [13] proposed a new digital image watermarking methodology: RSA and logistic asymmetric encryption methodology for robust embedding capacity and high computational efficiency. Generally, the scrambling parameters were stolen, when the information was converted on a public network, but the developed asymmetric encryption system effectively protects the parameters from attackers and hackers. In the experimental phase, the developed asymmetric methodology outperformed the other existing approaches by means of encryption time. In case, if the external key bit size was high in extracting procedure, the performance of the developed methodology gets degraded.

R.P. Singh, N. Dabas, and V. Chaudhary, [14] illustrated an effective watermarking methodology for securing and protecting the digital media information. In this research paper, a robust DWT watermarking methodology was implemented with Extreme Learning Machine (ELM), Online Sequential-ELM (OSELM) and Weighted-ELM (WELM) on different color images. The experimental outcome demonstrated that the developed watermarking methodology shows better result compared to other existing methodologies on different attacks such as, cropping, blurring, rotation, sharpening, scaling and scaling-cropping. The developed methodology performance was verified by using PSNR and BER. This literature does not concentrate on the contrast of reconstructed cover

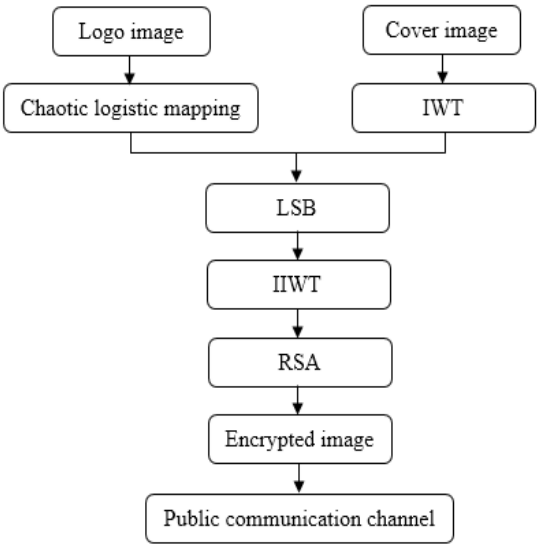


Figure.1 Encryption process

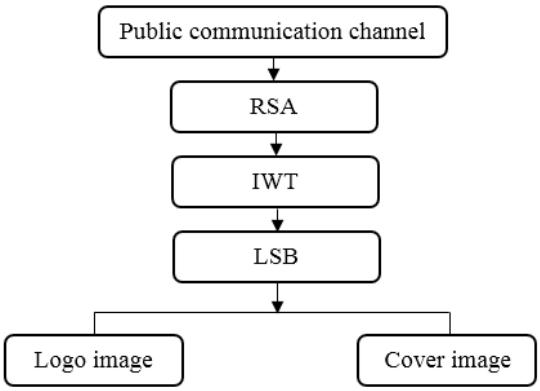
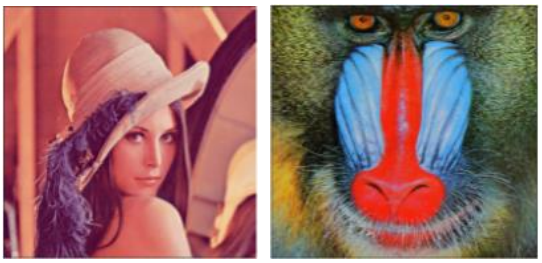


Figure.2 Decryption process

image, because it leads to the loss of information due to the changes in aspect ratio.

I.A. Ansari, M. Pant, and C.W. Ahn, [15] developed a robust watermarking system based on IWT and SVD. Normally, SVD method suffers with the problem of false positive issue, which leads to wrong owner authentication. To address this concern, IWT was used on the host image and then SVD was employed on the transformed image. This action helps to achieve high value of robustness. Additionally, an effective optimization method: ABC algorithm was used to further improve the quality of watermarking. In a large image dataset, the proposed watermarking system failed to achieve better decryption result by means of error rate.

To overcome the above mentioned drawbacks, an effective watermarking system is implemented for enhancing the security of transmission and information hiding process.



(a) (b)

Figure.3 Sample images: (a) Lena image and (b) baboon image

3. Proposed methodology

Image watermarking is the active research area in the field of information technology. In today's situation, watermarking is extensively utilized in communication systems that send secret information through appropriate carriers. In this scenario, the secret information that embeds in the cover image is named as logo image. The primary objective of this research paper is to develop a high level secure transmission technique to transmit messages through lossless channel. The proposed technique consists of four modules: IWT, chaotic logistic map, LSB and RSA process. The proposed methodology overcomes the drawback of existing techniques by the incorporation of IWT and chaotic logistic map for encryption. The working procedure of proposed technique is given in the Figs. 1 and 2.

3.1 Image acquisition

In the initial stage of watermarking, it is necessary to select appropriate digital image for watermarking, if the data is not acquired satisfactorily then the intended operations may not be achievable. In this research work, two digital images are preferred: Baboon and Lena as cover image [16]. The sample Lena and Baboon image is shown in the Fig. 3.

3.2 Integer wavelet transform

After considering the cover and logo image, the cover image is converted into transform domain by using the wavelet technique (IWT). In digital image watermarking, several wavelet techniques are used to hide the information. Mostly, the conventional wavelet techniques are leads to two concerns: content of the source media gets altered and cause distortion in the cover image. For example, in DWT, the input is given as an integer value, where the output doesn't effectively retrieve in the form of integer value, which causes restoration in the original cover image. The DWT uses floating point to hide the message, which causes data loss in the

original image. The floating point in the wavelet filter is persistent and it requires another process to remove the floating point. These limitations are avoided by using IWT and also it hides the information without causing distortion. So, IWT able to provide good visual system and also helps to improve the effectiveness of the system.

The IWT consists of four levels of sub-bands such as High-Low, Low-Low, Low-High and High-High. In this research study, Low-Low sub-band is considered, because it appears closely similar to the original image. The coefficients of IWT are shown in the below equations,

$$LL_{i,j} = |\frac{(Or_{2i,2j}+Or_{2i+1,2j})}{2}| \quad (1)$$

$$HL_{i,j} = Or_{2i+1,2j^-} - Or_{2i,2j} \quad (2)$$

$$LH_{i,j} = Or_{2i,2j+1} - Or_{2i,2j} \quad (3)$$

$$HH_{i,j} = Or_{2i+1,2J+1} - Or_{2i,2j} \quad (4)$$

The inverse transform is given as follows,

$$Or_{2i,2j} = LL_{i,j} - |\frac{HL_{i,j}}{2}| \quad (5)$$

$$Or_{2i,2j+1} = LL_{i,j} + |(HL_{i,j+1})/2| \quad (6)$$

$$Or_{2i+1,2j} = Or_{2i,2j+1} + LH_{i,j} - L_{i,j} \quad (7)$$

$$Or_{2i+1,2j+1} = Or_{2i+1,2j} + HH_{i,j} - LH_{i,j} \quad (8)$$

Where, $1 \le i \le \frac{X}{2}, 1 \le j \le Y/2$ and || is denoted as floor value, Or_i is stated as original images, X is denoted as height of the pixel and Y is represented as wide of the pixel. The level of each pixel is denoted as (i, j). Respectively, the logo image is encrypted by using a first level encryption technique: chaotic logistic mapping. In Fig. 4, the working process of IWT is clearly mentioned.

3.3 Chaotic logistic mapping

Generally, logistic map is a one dimensional chaotic mapping, which is widely used in various applications like multimedia data security, digital communication security, etc. Initially, the formula of logistic map is developed from the demographic feature, which is mathematically denoted in the Eq. (9).

$$X(k+1) = u \times X(k) \times [1 - X(k)],\ k = 0,1,2,3,..n \quad (9)$$

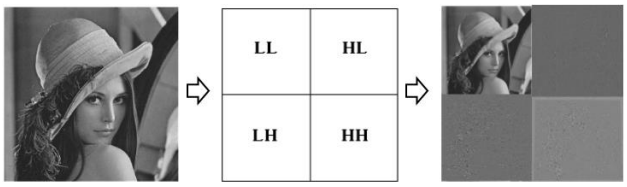


Figure.4 Working process of IWT

Where, $X(k)$ is represented as a mapping variable that ranges from$[0, 1]$. It helps to denote the ratio of existing population to the maximum possible population and u is denoted as a system parameter with the value of $u \in (0,4)$. This non-linear difference equation is intended to capture two effects; reproduction and starvation. Once the following two conditions are satisfied, then the logistic map function works in a mixed state, which is unpredictable and disorder way.

$$0 < X(0) < 1,\ 3.569945 < u < 4 \quad (10)$$

In order to obtain a one-dimensional sequence, it is essential to iterate $m \times n$ times, when an image of $m \times n$ is encrypted. The obtained sequence is normalized and a new sequence is generated in the range of (0,255). The new sequence is transformed into two dimensional matrix, which is named as encrypted image matrix. This process helps to achieve a high level of security, while encrypting a logo image with logistic map. The sequences generated by the developed encryption function are irrelevant, aperiodic and non-convergent. Furthermore, the developed encryption function is very sensitive to initial values, even if the initial conditions are quite close. Also, the iteration outcomes are not similar and the uncorrelated chaotic sequence numbers are very large. So, it is very tough for attackers to determine the exact initial condition of the chaotic system from a finite length sequence.

3.4 Least significant bit

After encryption and transformation, the pixel values of logo image and cover image is converted into binary values by using 8-bit LSB. The size of cover image is represented as $m \times n$ and the size of logo image is denoted as $m \times n/8$. The eighth bit of cover image is replaced by each bit of logo image [17]. In this way, the logo image is embedded into the cover image. Fig. 5 represents the process of LSB watermarking using 8-th bit. The respective eight bit values of watermarked image are converted into decimal number. Then, inverse-IWT is performed on the decimal number, the resultant image is given as the input for RSA algorithm.

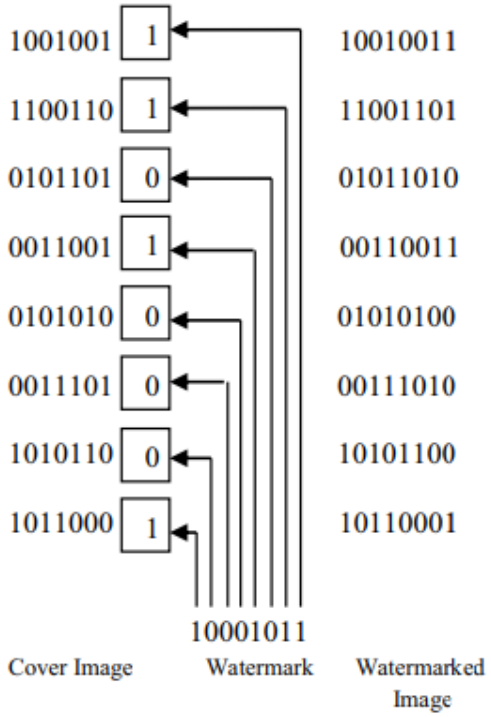


Figure.5 Process of LSB watermarking using 8-th bit

3.5 Rivest–Shamir–Adleman algorithm

A second level encryption technique: RSA algorithm is employed for encrypting the resultant inverse-IWT image, which is one of the popular watermarking cryptographic system. It is used for security purpose in the wide range of networks. The public and private key-generation is the most essential part of RSA algorithm. The public key encryption system uses an asymmetric encryption mechanism for protecting the encrypted data by using a pair of keys. The RSA algorithm belongs to the block-cipher domain, the detailed process of key generation is given below,

- Two large prime numbers m and n are randomly generated.
- Evaluate Euler's totient function $\varphi(N)$ and one secret key member N by using the Eq. (11).

$$N = m \times n, \quad \varphi(N) = (m-1) \times (n-1) \quad (11)$$

- Randomly select an encryption key by satisfying the below condition, which is mathematically mentioned in the Eq. (12). This logic expression presents the great common divisor between $\varphi(N)$ and e, which are considered as co-primes.

$$1 < e < \varphi(N), \gcd\big(e, \varphi(N)\big) = 1 \quad (12)$$

- Evaluate the decryption key d by using the Eq. (13).

$$e \times d = 1 mod \varphi(N), 0 \leq d \leq N \quad (13)$$

In public key system, there are two types of public key, private key and secrete key are generated, which are in the form of (d, N) and (e, N), respectively. The public key is known to all and the private key is kept secret. In data transmission, the sender knows the recipient of public key and then encrypts the message by using the private key. After generating the cipher text, the sender transmits the cipher text to the receiver. Then, the receiver processes the cipher text by using the private key and gets the plain secrete message. This action ensures the security of the RSA encryption system. Though, attackers knows the public key for e and N, because it is open to the public. Whereas, N is denoted as great number and e is represented as random number. Thus, it is difficult for the attackers to know the values of m and n by large integer factorization, which is known as non-deterministic polynomial time hard issue. Finally, the encrypted RSA image is transferred through lossless channel, where the receiver retrieves the embedded logo image by using the decryption process.

3.6 Decryption module

Once the embedding process is over, the extraction process is carried out on the encrypted RSA image to retrieve the logo image from cover image. The decryption module is a single stage process, which is opposite to the encryption process. Subsequently, the IWT and LSB processes are executed in the encrypted image after performing RSA algorithm. The decrypted image should be the exact copy of the original logo image. The work flow of decryption module is given in the Fig. 2.

4. Experimental result and discussion

In this section, experimental result and discussion of the proposed methodology is detailed effectively and also described about the experimental set-up and performance measure. The performance of the proposed methodology was evaluated by means of comparative and quantitative analysis.

4.1 Experimental setup

The proposed methodology was experimented by using MATLAB (version 2017a) with 4 GB

RAM, 3.0 GHz Intel i3 processor and 500 GB hard disc. In order to estimate the efficiency of proposed algorithm, the proposed methodology performance was compared with other existing studies. In this research paper, size of the cover image is 512×512 and size of the logo image is 256×256. The performance evaluation of proposed methodology was also done under the circumstance of noise attack by means of PSNR and entropy.

4.2 Performance measure

Performance evaluation is defined as regular measurement of results and outcomes that develops reliable information about the efficiency and effectiveness of programs. In this research, entropy value and PSNR parameters are employed for comparing the performance evaluation of input and decrypted image. PSNR is most easily defined by Mean Squared Error (MSE), MSE is mathematically represented in the Eq. (14),

$$MSE = 1/mn \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(x,y) - k(x,y)]^2 \quad (14)$$

Where, $m\ and\ n$ are stated as an image and $I(x,y)$ is defined as input image, $k(x,y)$ is represented as decrypted image. Another criterion, which is used for evaluating the PSNR value is given the Eq. (15),

$$PSNR = 10\ log_{10}(\frac{255^2}{MSE}) \quad (15)$$

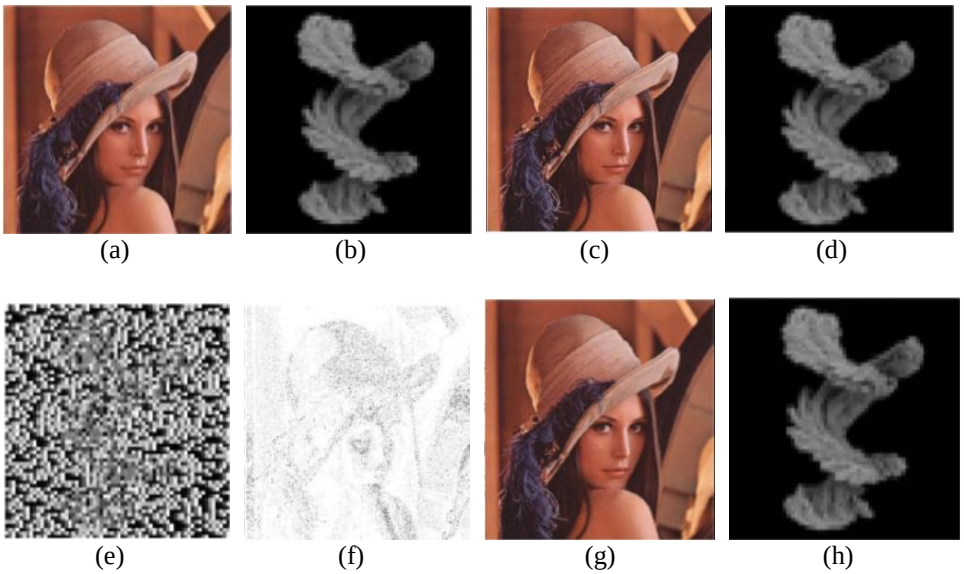
Additionally, effectiveness of the proposed methodology is further analyzed based on the entropy calculation. The entropy $E(m)$ of a message m is measured by using the Eq. (16),

$$E(m) = \sum_{i=0}^{m-1} p(m_i) log_2 \frac{1}{p(m_i)} \quad (16)$$

Where, m is denoted as total number of symbols $m_i \epsilon m$ and $p(m_i)$ is denoted as the probability of symbol occurrence m_i.

4.3 Experimental analysis on color image

This sub-section demonstrates the experimental analysis of color image. Fig. 6 exhibits the color image that undertaken for image embedding and extracting process. Fig. 6 (a) denotes the Lena image, which is considered as cover image. Fig. 6 (b) represents the logo image that is considered as secrete image. The IWT cover image is achieved by applying IWT wavelet method, which is shown in the Fig. 6 (c). The chaotic logistic mapped color logo image is shown in the Fig. 6 (d). The LSB is performed on the chaotic logistic mapped logo image and encrypted Lena image, which is shown in the Fig. 6 (e). The Fig. 6 (f) denotes the encrypted image after executing RSA encryption algorithm in the LSB image. The final decrypted color image is shown in the Fig. 6 (g) and 6 (h). Additionally, the histogram representations of color image is denoted in the Fig. 7.



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure.6 Color images: (a) color cover image 512×512, (b) logo image 256×256, (c) IWT-cover image, (d) chaotic logistic mapped logo image, (e) LSB image, (f) RSA encrypted image, (g) decrypted cover image, and (h) decrypted logo image

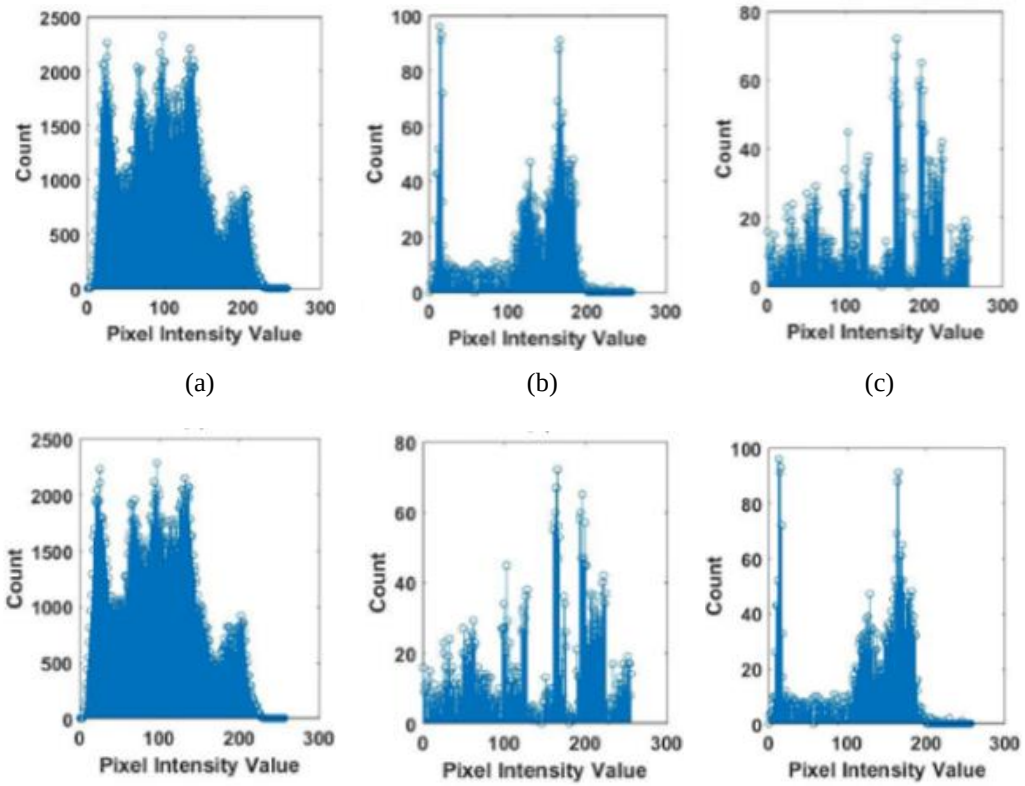


Figure.7 Histogram diagram of color image: (a) cover image, (b) logo image, (c) RSA encryption, (d) encrypted image, (e) RSA decryption, and (f) decrypted image

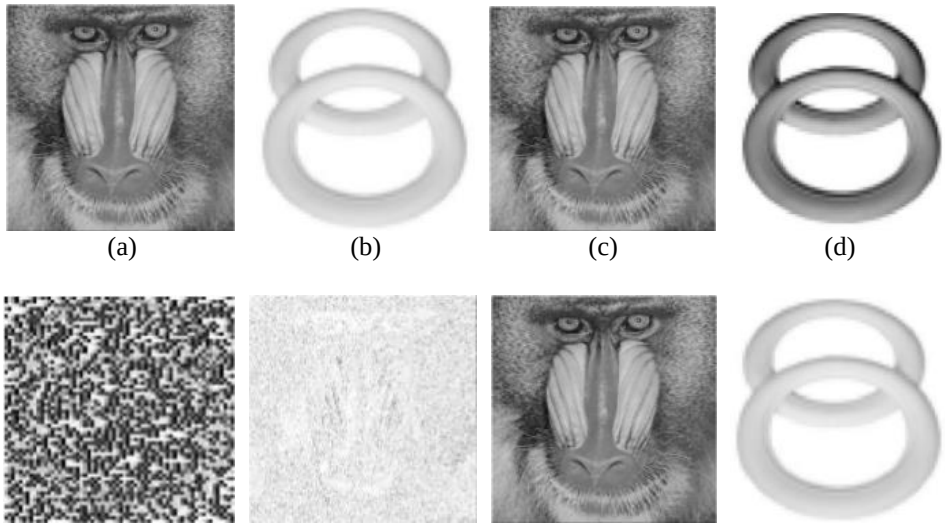
Table 1 demonstrates the performance of proposed methodologies: IWT-chaotic logistic mapping algorithm for color image. In this scenario, the evaluation is done in two ways: normal color image, and noisy color image (adding 10% and 20% of salt and pepper noise). The proposed technique delivers 36.5119 dB of PSNR and 7.8914 of entropy value in the normal color image. Consequently, the proposed technique achieves 52.56 dB of PSNR and 7.63 of entropy value in the noisy color image (adding 10% of salt and pepper noise). In addition, the proposed technique achieves 36.39 dB of PSNR and 7.562 of entropy value in the noisy color image (adding 20% of salt and pepper noise)

Table 1. Performance evaluation of color image

Methodology	**Performance measure**	**Normal color image**	**Noisy color image**	
			10%	**20%**
IWT-Chaotic logistic mapping	PSNR (dB)	36.5119	52.56	36.39
	Entropy	7.8914	7.63	7.562

4.4 Experimental analysis on grayscale image

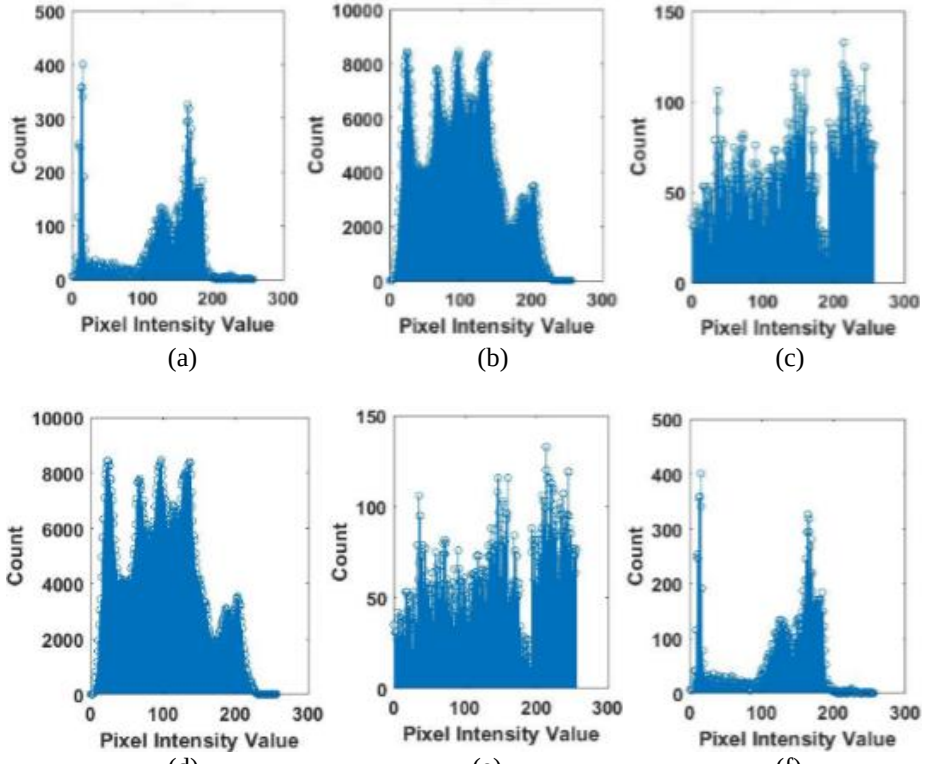
This section demonstrates the experimental analysis of grayscale image. The Fig. 8 (a) represents the input grayscale baboon image, which is used as a cover image. Respectively, Fig. 8 (b) represents the logo image that is considered as a secret image. Fig. 8 (c) shows IWT cover image, which is obtained after performing IWT in the cover image. The chaotic logistic mapped logo image is shown in the Fig. 8 (d). The LSB is applied in the chaotic logistic mapped logo image and encrypted baboon image, which is graphically shown in the Fig. 8 (e). The Fig. 8 (f) represents the encrypted image after performing RSA encryption algorithm in the LSB image. The final decrypted image is shown in the Fig. 8 (g) and 8 (h). The histogram representations of grayscale image are specified in the Fig. 9.



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure.8 Grayscale images: (a) grayscale cover image 512×512, (b) logo image 256×256, (c) IWT-cover image, (d) chaotic logistic mapped logo image, (e) LSB image, (f) RSA encrypted image, (g) decrypted cover image, and (h) decrypted logo image



(a) (b) (c)

(d) (e) (f)

Figure.9 Histogram diagram of grayscale image: (a) cover image, (b) logo image, (c) RSA encryption, (d) encrypted image, (e) RSA decryption, and (f) decrypted image

In Table 2, the performance evaluation of proposed methodology is validated by means of PSNR and entropy value. In this section, the evaluation is done in two ways: normal grayscale image, and noisy grayscale image (adding 10% and 20% of salt and pepper noise). The proposed technique delivers 36.2512 dB of PSNR and 7.1432 of entropy value in the normal grayscale image. In addition, the proposed technique achieves 55.67 dB of PSNR and 7.57 of entropy value in the noisy grayscale image (adding 10% of salt and pepper noise). Consequently, the proposed technique achieves 34.3765 dB of PSNR and 7.5385 of entropy value in the noisy grayscale image (adding 20% of salt and pepper noise).

Table 2. Performance evaluation of grayscale image

Methodology	Performance measure	Normal grayscale image	Noisy grayscale image	
			10%	20%
IWT-Chaotic logistic mapping	PSNR (dB)	36.2512	55.67	34.3765
	Entropy	7.1432	7.57	7.5385

Table 3. Comparative analysis of proposed and existing methodologies

Methods	Images	PSNR (dB)	Entropy value
DCT + Arnold transform [18]	Color image	10.31405	7.06755
DWT-SVD + SDE algorithm [19]	Grayscale image	34.28085	-
Hybrid Fractal-Chaos algorithm [20]	Color image	-	7.5937
RWT+SVD +GA [21]	Grayscale image (adding salt and pepper noise)	50.5246	-
IWT-Chaotic logistic mapping	Color image	36.5119	7.8914
	Grayscale image	36.2512	7.1432
	Grayscale image (adding 10% salt and pepper noise)	55.67	7.57

4.5 Comparative analysis

Table 3 represents the comparative study of existing work and the proposed work performance. K. Naik, and A.K. Pal, [18] developed an effective image cryptosystem for an uncompressed color image by using DCT for selecting the superior coefficients. These coefficients were applied in the encryption process for decreasing the computational overhead. Then, the selected coefficients were confused by using Arnold transform followed by diffusion with keys. After completion of the encryption process, unencrypted coefficients were appended with encrypted components to form an uncompressed encrypted image. The developed scheme was tested on a set of standard color images and a satisfactory result was attained with the entropy value of 7.06755 and PSNR of 10.31405 dB.

Additionally, M. Ali, and C.W. Ahn, [19] presented an optimal wavelet domain (DWT-SVD) for image watermarking by using Self-Adaptive Differential Evaluation (SDE) algorithm. In this research paper, two level DWT was employed on the cover image, and then SVD was applied to every sub-band at second level of DWT. The scaled components were inserted into the singular value matrix of the host image. The scaling factors were optimized by using SDE algorithm for obtaining better imperceptibility with highest possible robustness. The developed methodology achieved 34.28085 dB of PSNR in grayscale Lena image. Compared to these existing studies, the proposed method works effectively in terms of PSNR and entropy value. In the proposed research, a two level encryption was performed (chaotic logistic mapping with RSA) with IWT and 8-bit LSB. The advantage of proposed methodology was highly secure and safe for its users by using complex mathematics. It was tough to crack, because it involves factorization of large prime number that were difficult to factorize.

S.R.M. Halagowda, and S.K. Lakshminarayana, [20] developed a hybrid encryption technique for delivering high secure transmission. Here, image encryption and decryption process was done by employing hybrid fractal-chaos technique. The developed methodology consists of four modules; key generation, fractal encryption, chaos encryption and decryption. Initially, a key was generated for encrypting and decrypting the image or data. Consequently, fractal-image encryption was carried out by applying L-shaped tromino. Likewise, chaos encryption was done by employing DCT to achieve the final encrypted image. Whereas, decryption process was performed using chaos decryption and fractal decryption algorithms.

N.N. Mood, and V.S. Konkula [21] developed an intelligent, robust and secure watermarking method on the basis of Redundant Wavelet Transform (RWT), SVD and Genetic Algorithm (GA). The developed watermarking scheme accomplished RWT and SVD for feature extraction and the GA for optimization. Additionally, the developed method created a signature embedding mechanism in which the watermarked image will be more secure. Compared to these existing research papers, the proposed technique achieved better result by means of PSNR and entropy value.

5. Conclusion

In this scenario, an effective watermarking methodology is developed based on the objectives to improve the robustness and imperceptibility. At first,

IWT-chaotic logistic mapping is used to transform the logo and cover image into wavelet domain. For embedding the logo image in cover image, a simple methodology: LSB is undertaken, which alters the bit value of cover image for hiding the logo image. Then, asymmetric encryption algorithm (RSA) is carried out on the LSB image for enhancing the hidden data security with good embedding capacity and high computational efficiency. Once the encryption process is over, then the decryption procedure is accomplished to retrieve the original logo image from the cover image. Compared to the other obtainable schemes, the proposed methodology delivers an effective performance by means of PSNR and entropy value. The proposed methodology almost achieved 19 dB enhancement in PSNR and 0.07-0.7 improvement in entropy value than the previous methods. In future work, an efficient optimization algorithm is utilized for further enhancing the efficiency of proposed methodology performance.

References

[1] S. Roy and A.K. Pal, "A blind DCT based color watermarking algorithm for embedding multiple watermarks", *AEU-International Journal of Electronics and Communications*, Vol.72, pp.149-161, 2017.

[2] S.P. Singh and G. Bhatnagar, "A new robust watermarking system in integer DCT domain", *Journal of Visual Communication and Image Representation*, Vol.53, pp.86-101, 2018.

[3] R.A. Alotaibi and L.A. Elrefaei, "Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT)", *Applied Computing and Informatics*, In Press, 2018.

[4] J. Abraham and V. Paul, "An imperceptible spatial domain color image watermarking scheme", *Journal of King Saud University-Computer and Information Sciences*, In Press, 2016.

[5] Y. Gangadhar, V.G. Akula, and P.C. Reddy, "An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation", *Biomedical Signal Processing and Control*, Vol.43, pp.31-40, 2018.

[6] N. Tiwari, "Digital Watermarking Applications, Parameter Measures and Techniques", *International Journal of Computer Science and Network Security*, Vol.17, No.3, pp.184, 2017.

[7] M.H. Vali, A. Aghagolzadeh, and Y. Caleigh, "Optimized watermarking technique using self-adaptive differential evolution based on redundant discrete wavelet transform and singular value decomposition", *Expert Systems with Applications*, Vol.114, pp.296-312, 2018.

[8] M. Malonia and S.K. Agarwal, "Digital image watermarking using discrete wavelet transform and arithmetic progression technique", In: *Proc. of International Conf. on Electrical, Electronics and Computer Science*, pp.1-6, 2016.

[9] H.A. Abdallah, R.A. Ghazy, H. Kasban, O.S. Faragallah, A.A. Shaalan, M.M. Hadhoud, M.I. Dessouky, N.A. El-Fishawy, S.A. Alshebeili, and F.E.A. El-Samie, "Homomorphic image watermarking with a singular value decomposition algorithm", *Information Processing & Management*, Vol.50, No.6, pp.909-923, 2014.

[10] V.S. Verma, R.K. Jha, and A. Ojha, "Significant region based robust watermarking scheme in lifting wavelet transform domain", *Expert Systems with Applications*, Vol.42, No.21, pp.8184-8197, 2015.

[11] I.A. Ansari and M. Pant, "Multipurpose image watermarking in the domain of DWT based on SVD and ABC", *Pattern Recognition Letters*, Vol.94, pp.228-236, 2017.

[12] H.T. Hu and L.Y. Hsu, "Collective blind image watermarking in DWT-DCT domain with adaptive embedding strength governed by quality metrics", *Multimedia Tools and Applications*, Vol.76, No.5, pp.6575-6594, 2017.

[13] Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, "Secure and robust digital image watermarking scheme using logistic and RSA encryption", *Expert Systems with Applications*, Vol.97, pp.95-105, 2018.

[14] R.P. Singh, N. Dabas, and V. Chaudhary, "Online sequential extreme learning machine for watermarking in DWT domain", *Neuro-Computing*, Vol.174, pp.238-249, 2016.

[15] I.A. Ansari, M. Pant, and C.W. Ahn, "Robust and false positive free watermarking in IWT domain using SVD and ABC", *Engineering Applications of Artificial Intelligence*, Vol.49, pp.114-125, 2016.

[16] B. Escalante-Ramírez and S.L. Gomez-Coronel, "A Perceptive Approach to Digital Image Watermarking Using a Brightness Model and the Hermite Transform", *Mathematical Problems in Engineering*, Vol. 2018, 2018.

[17] N. Bansal, V.K. Deolia, A. Bansal, and P. Pathak, "Digital image watermarking using least significant bit technique in different bit positions", In: *Proc. of International Conf. on*

Computational Intelligence and Communication Networks, pp.813-818, 2014.

[18] K. Naik and A.K. Pal, "A Partial Image Cryptosystem Based on Discrete Cosine Transform and Arnold Transform", In: *Proc. of International Conf. on Recent Advances in Information Technology*, New Delhi, pp.65-73, 2014.

[19] M. Ali and C.W. Ahn, "An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain", *Signal Processing*, Vol.94, pp.545-556, 2014.

[20] S.R.M. Halagowda and S.K. Lakshminarayana, "Image Encryption Method based on Hybrid Fractal-Chaos Algorithm", *International Journal of Intelligent Engineering and Systems*, Vol.10, No.6, pp.221-229, 2017.

[21] N.N. Mood and V.S. Konkula, "A Novel Image Watermarking Scheme Based on Wavelet Transform and Genetic Algorithm", *International Journal of Intelligent Engineering and Systems*, Vol.11, No.3, pp.251-260, 2018.