Hybrid Image Encryption using Advanced Encryption Standard and Chaos Encryption with Chaotic Tent Map

T. Venugopal[1], Dr. V. Siva Kumar Reddy[2]
[1] *Research Scholar, Rayalaseema University, Kurnool, A.P., India*
[2]*Principal, Malla Reddy College of Engineering and Technology, Hyderabad, Telangana, India*
(E-mail: tipirneni.venu@gmail.com)

***Abstract*—** Image cryptography is one of the growing research area in the field of information technology. Currently, cryptography is extensively used in communication systems that send and receive secret data/information through appropriate carriers. In recent decades, numerous image cryptography algorithms are developed such as, blowfish, two fish, fractal encryption, etc. These algorithms have many inevitable issues like slow learning, poor computational capability, etc. To overcome these issues, a new hybrid image encryption algorithm is proposed in this research paper. Here, the hybrid image encryption algorithm includes chaos encryption with chaotic tent map and Advanced Encryption Standard (AES) (128 bit) encryption method. The experimental results confirm that the proposed algorithm develops a secure transmission network with low computational complexity in light of entropy value, Peak Signal-to-Noise Ratio (PSNR), and Unified Averaged Changed Intensity (UACI). Compared to other existing methods, the proposed algorithm improved PSNR value up to 2-9 dB, entropy value up to 0.15, and UACI value up to 6.2%.

Keywords*—Advanced encryption standard; chaos encryption with chaotic tent map; Integer wavelet transform; Least significant bit.*

I. INTRODUCTION

In recent periods, the rapid growth in digital contents (images, texts, videos, etc.) and industrial communication technology leads to the high need of information security [1-2]. Presently, most of the applications need a level of security to be safely utilized in different communication channels [3]. Additionally, the digital information privacy and information secrecy has become one of the most important issues that force information technology experts to develop innovative methodologies for securing and protecting the information. Furthermore, the vast usage of networking technology in all over the daily needs makes the information security a significant concern for researchers to develop a new methodology [4-5]. To secure and protect the secret information against unauthorized users a need has emerged to use many types of encryption approaches; optical multiple-image encryption [6], chaos encryption [7], hybrid encryption [8], etc. So, the cryptography image encryption plays an important role in protecting the images sent and received over the pay television, mobile phones, private emails, e-commerce, etc. [9-10]. Generally, there are two categories of cryptography algorithms such as, symmetric encryption and asymmetric encryption. In symmetric encryption, a same key is utilized for both encryption and decryption and in asymmetric encryption different keys are used for encryption and decryption. Asymmetric encryption algorithms are more secure, while comparing with symmetric encryption algorithms.

The main aim of this research work is to present an efficient, flexible and highly secure system for data transmission. In this research, a hybrid encryption algorithm (Chaos encryption with chaotic tent map and AES encryption) was developed for secure data transmission with low computational complexity. Here, an appropriate transformation approach: Integer Wavelet Transform (IWT) is applied to the cover image, before embedding the secret image in the cover image. Compared to other wavelet transforms, IWT effectively decreases the data loss in the extracted secret and cover images. Subsequently, chaos encryption with the chaotic tent map is applied to the secret image, before embedding the secret image in the cover image. Chaos encryption with chaotic tent map prevents the loss of information and also provides a good data safety assurance that enhances the security of data/information transmission. In addition, chaos encryption generates the position of pixels for embedding process. While embedding, the Least Significant Bit (LSB) was the bit position of the integer unit value. After embedding the secret image in cover image, another encryption algorithm (AES encryption) is applied to encrypt the digital images. For assessing the proposed algorithm performance, a few parameters were under-taken for experimental analysis.

This research paper is organized as follows. Several recent papers in image encryption are reviewed in the section II. Detailed explanation about the proposed algorithm (Chaos encryption with chaotic tent map-AES encryption) is given in the section III. Section VI illustrates about the quantitative analysis and comparative analysis of proposed algorithm. Conclusion is made in the Section V.

II. LITERATURE REVIEW

Several methods have been developed by the researchers on image encryption and decryption. In this sub-section, a brief evaluation of a few essential contributions to the existing literature papers are presented.

X. Wang, et al. [11] developed a new system (one-time pad approach) for chaotic image encryption, which works on the basis of cyclic shift function and multiple mixed hash function.

Here, the initial values were generated using both information of the chaotic sequence and the plaintext image, which were determined using MD5 and SHA1 hash models. In addition, the scrambling sequences were generated by the logistic map and nonlinear equation. This research paper rectifies the problems of traditional Baptista systems. At last, the piecewise linear chaotic maps and cyclic-shift function were applied for diffusing the image. The experimental outcome showed that the developed system provides better security and also resist different attacks. The major drawbacks of this system are the poor quality of the recovered images and heavy computation cost.

A. Daneshgar, and B. Khadem, [12] presented a new methodology: word based chaotic image encryption scheme for grayscale image encryption and decryption, which was utilized in both self-synchronous and synchronous modes. The developed encryption approach works in the finite field, where its performance was analysed based on the numerical precision. In this literature paper, the developed encryption approach not only passes a variety of security tests, and also it was verified that the developed encryption approach works faster than other existing approaches of the same type even while utilizing light-weight short key sizes. The performance of high capacity based image encryption approaches gets degraded, if the external key bit size was high in extracting and embedding processes.

C. Pak, and L. Huang, [13] developed an effective and simple system by utilizing the output sequences of three existing one dimensional (1D) chaotic maps (sine map, Chebyshev map, and logistic map). Performance evaluation and the experimental simulation showed that the developed system produced a 1D chaotic system with good chaotic performance and higher chaotic ranges associated to the existing chaotic maps. In this literature paper, the experimental evaluation was performed on the developed system using key sensitivity analysis, key space analysis, several statistical analyses, and differential analysis. The experimental consequences showed that the developed system delivered a better security level with low computational complexity. In this research study, the decrypted image should be equal to the original image, which was considered as one of the major concerns in the developed system.

X. Zhang, et al. [14] presented a new hierarchical image encryption algorithm based on vector stochastic decomposition method and cascaded interference structure. By using these methods, the secret images were modulated by a random phase distribution and then encoded into a phase only mask key. In this research study, the decryption occurs only when the high-level users con-currently find the correct geometrical parameters, correct phase keys, and correct sequential orders of phase keys. Finally, both the theoretical and experimental simulations verified the feasibility of the developed algorithm. The developed hierarchical image encryption algorithm was only useful, when the region of interest or area was known and also the phase only mask key was not secure in transformation.

H. Li, et al. [15] developed a new chaos based image encryption system based on dynamic state variable selection and orbit perturbation. In this research paper, two dimensional logistic adjusted sine map was applied for generating the pseudo random numbers. By using an auxiliary value, the chaotic map orbit was continuously perturbed by the earlier processed pixels and then one of the two state values was selected for generating the key-stream. Subsequently, the key-stream works on the basis of control parameter of the chaotic map and information of the cipher and plain images. A number of simulations were performed for verifying the security and effectiveness of the developed system. Here, it was very difficult to intruder for retrieving the original image without knowing the similarity between original and encrypted images.

To address the above mentioned problems, an effective image encryption approach is developed for improving the information hiding process and security of transmission.

III. PROPOSED METHODOLOGY

In current scenario, computer has become an essential device that helps to store and transmit data/information from one location to another location. The information that is shared must be transferred in a secured manner. So, the data is encrypted into unreadable formats by an authorized person for ensuring the secured transmission of information. Image cryptography is the science of information security that becomes a very crucial aspect of modern computing systems towards securing data storage and transmission. In this research study, the proposed encryption algorithm consists of six phases; image collection, IWT, chaos encryption with tend map, LSB, AES encryption algorithm, and decryption phase. Fig. 1 shows the work flow of the proposed encryption algorithm. The explanation about the proposed encryption algorithm is described below.

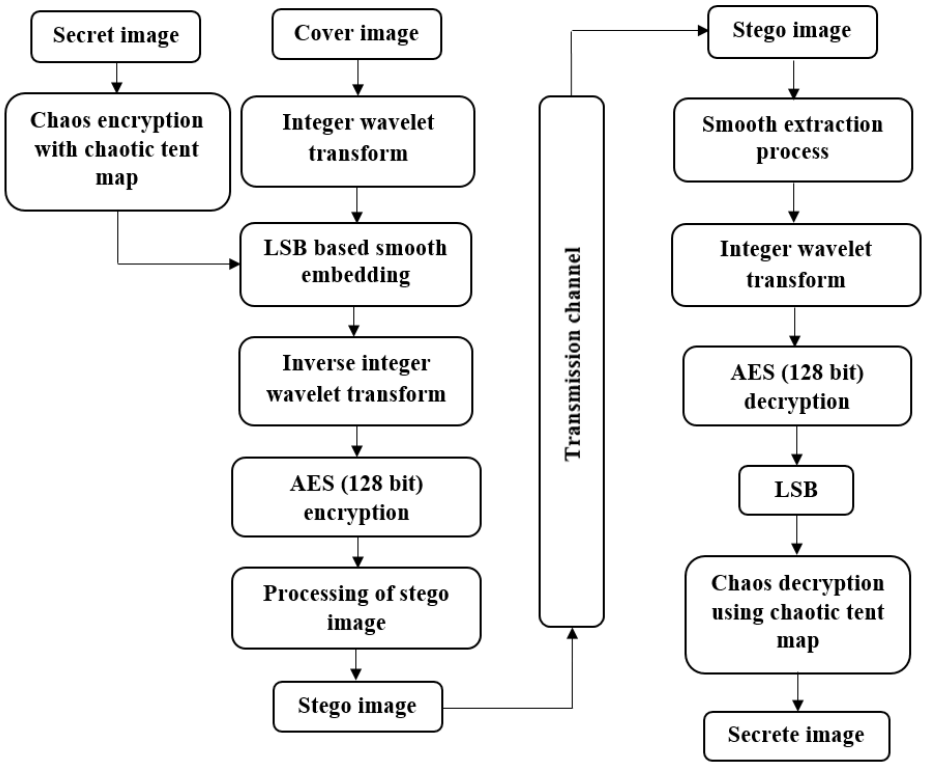

Fig. 1: Work flow of proposed methodology

A. Image collection

In image cryptography, two types of images (cover image and secret image) are utilized for experimental investigation. Generally, the cover image is used for embedding the secret image that should be noiseless and appropriate image. This research study has considered total four digital images such as, baboon, Lena, boat, and couple. In that, baboon and Lena are colour images, boat and couple are grayscale images. The sample digital images are graphically represented in the Fig. 2.

Fig. 2: Sample collected digital images

B. Integer wavelet transform

After collecting the digital images, the cover image is converted into transform domain by applying IWT approach. Usually, the IWT method comprises of four levels of sub-bands; 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 represented in the Eq. (1), (2), (3), and (4).

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

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

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

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

Likewise, the coefficients of inverse-IWT are represented in the Eq. (5), (6), (7), and (8).

$$O_{2i,2j} = LL_{i,j} - \left| \frac{HL_{i,j+1}}{2} \right| \quad (5)$$

$$O_{2i,2j} = LL_{i,j} + \left| \left(HL_{i,j+1}\right) \Big/ 2 \right| \quad (6)$$

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

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

Where, the level of each and every image pixel is represented as $(i, j), O_i$ is specified as the original image, X is indicated as the height of image pixel, Y is denoted as the width of image pixel and $1 \le i \le \frac{X}{2}, and\, 1 \le j \le \frac{Y}{2}$ are represented as the floor values.

C. Chaos encryption with tend map

Currently, chaos encryption algorithms have wide reputation among researchers, because of its inherent features of chaos systems. Usually, the chaos image cryptosystem comprises of two phases; permutation and diffusion. In the diffusion phase, each pixel values are altered by applying chaos sequences. Respectively, in the permutation phase, the pixel permutation was considered as the position of image pixels that are scrambled over the entire image without disturbing the value of image pixels. In this research, the diffusion and permutation phases are performed by using the generated keys K_i and the value of tend map. In chaos encryption, one of the simplest chaotic maps is tend map, which is mathematically given in the equation (9).

$$T(r, X_n) = \begin{cases} RX_n/2 & if\ X_n < 0.5 \\ R(1-X_n)/2 & if\ X_n \ge 0.5 \end{cases} \quad (9)$$

Where, X_n is represented as the chaos sequence that ranges between [0, 1] and R is stated as positive parameter that ranges $R \in (3.57, 4)$

Then, iterate the tend map for five times in order to accomplish rid of the transient effect by using the parameter value of tend map and generated keys K_i. Besides, sort the chaotic orbit that obtained from the prior steps and then permutated the diffused or plain-image using the Eq. (10).

$$mim(i) = permut \oplus K_i\left(tend\ p(i)\right) \square\ i = 1, 2, 3, ...m \times n \quad (10)$$

Where, m and n are represented as the width and height of the plain-image, $p(i)$ is denoted as the original image pixel value, $mim(i)$ is denoted as the pixel value. At last, generate the cipher key for permuted image and then diffuse the plain or permuted image by using tend chaotic orbit. The output of diffusion stage is cipher-image, which is mathematically represented in the Eq. (11).

$$c(i) = mim(i), i = 1, 2, 3, ...m \times n \quad (11)$$

D. Least significant bit

After cover image transformation and secret image encryption, embedding mechanism is carried-out for hiding the secret image in cover image. In embedding process, LSB is used as the bit position of the integer unit value. Here, the pixel values of cover and secret images are transformed into binary values by applying eight bit LSB. In this research study, the size of secret image is represented as $m \times n/8$ and the size of cover image is denoted as $m \times n$. In eight bit LSB, the eight bit of cover image is interchanged with each and every bit of secret image. In this manner, the secret image is embedded into the cover image. Then, the binary values are converted into decimal numbers. Besides, inverse-IWT is accomplished on the decimal numbers, the respective output image is given as the input for AES (128 bit) encryption algorithm.

E. AES encryption algorithm

AES is an iterative encryption algorithm, which encrypts and decrypts the data on the basis of Substitution and Permutation Network (SPN). The SPN is a number of mathematical operations, which are performed in block cipher algorithms. The AES encryption algorithm has the ability to deal with 128 bits (16 bytes) as a fixed plain text block size. The respective 128 bits are denoted as 4×4 matrix, where it operates on a matrix of bytes. Basically, the AES encryption algorithm comprises of four phases; substitute bytes' transformation, shift-rows transformation, mix-columns transformation, and add-round key transformation. The substitute bytes' transformation phase depends on non-linear S-box for substituting a byte in the state of another byte. The main idea of next phase (shift-rows transformation) is to shift the bytes to the left side of every row. In this phase, the bytes of row number remain zero and also it does not carry any permutation. Here, only one byte is shifted circular to left in the first row, two bytes are shifted circular to left in the second row, and three bytes are shifted circular to left in the last row. The size of new state remains unchanged, but the position of the bytes is shifted.

Another important phase in AES algorithm is mix-columns transformation. Here, each byte of one row in matrix transformation is multiplied with each value (byte) of the state column. In another word, each row of matrix transformation is multiplied with each column of the state. The outcomes of these multiplication are XOR for producing a new four bytes for the next state. In this phase, the size of state remains unchanged with the original size of 4×4. Furthermore, add-round key transformation is the most vital phase in AES algorithm. In this phase, both the input data and the key are structured in a 4×4 matrix of bytes. The add-round key transformation has the ability to provide high security, while encrypting the data. This operation is based on creating the relationship between the cipher text and the key.

F. Decryption phase

After embedding process, the extraction process is performed on the AES encrypted stego image for retrieving the secret image from the cover image. In this research study, the decryption phase is a single stage process that is directly

proportional to the encryption phase. Here, AES decryption algorithm and chaos decryption using chaotic tent map are applied subsequently in order to extract the secret image from the cover image. The extracted secret image must be the exact copy of the original secret image.

IV. EXPERIMENTAL RESULT AND DISCUSSION

In this experimental section, the proposed methodology was simulated using MATLAB (version 2018a) with 3.0 GHZ-Intel i5 processor, 1TB hard disc, and 8 GB RAM. The proposed methodology performance was compared with other existing methodologies for estimating the efficiency and effectiveness of the proposed encryption algorithm. The performance evaluation of proposed encryption algorithm was also done under the circumstance of noise attacks (Salt and Pepper (SP) noise, Gaussian noise), and crop attacks. The performance of proposed encryption algorithm was validated in light of entropy value, PSNR, and UACI. Here, the size of cover image was 256×256 and the size of secret image was 128×128.

A. Performance measure

Performance measure is defined as the regular measurement of outcomes and results that develops a reliable information about the effectiveness of proposed encryption algorithm. Also, performance measure is the procedure of reporting, collecting and analysing information about the performance of a group or individual. The mathematical equation of an entropy value, PSNR, and UACI are represented in the Eq. (12), (13), (14) and (15), respectively.

$$E(m)=\sum_{i=0}^{m-1}p(m_i)\log_2\frac{1}{p(m_i)} \tag{12}$$

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

$$PSNR=10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{13}$$

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

Where, m *and* n are represented as width and height of the image, $k(x,y)$ is denoted as the decrypted image, and $I(x,y)$ is indicated as the input image.

$$UACI=\frac{1}{MN}\sum_{i=1}^{M}\sum_{J=1}^{M}\frac{\left|C_1(i,j)-C_2(i,j)\right|}{255}\times100 \tag{15}$$

Where, N and M are represented as the height and width of the image, and C_1 and C_2 are denoted as the encrypted image.

B. Quantitative analysis on colour images

The experimental analysis of colour images is demonstrated in this sub-section. Here, Fig. 3 represents the colour images (Lena and baboon) that are under-taken for image embedding and extracting process. Fig. 3(a) represents cover image (baboon) and Fig. 3(b) denotes secret image (Lena). The image after applying IWT in cover image is denoted in the Fig. 3(c). Likewise, the image after applying chaos encryption with chaotic tent map in secret image is illustrated in the figure 3(d). The embedded encrypted secret image and transformed colour image is denoted in the Fig. 3(e). Fig. 3(f) represents the encrypted image after performing AES encryption algorithm in the embedded image. The final decrypted colour and secret images are shown in the Fig. 3(g) and 3(h). In addition, the histogram representations of colour image are indicated in the Fig. 4.

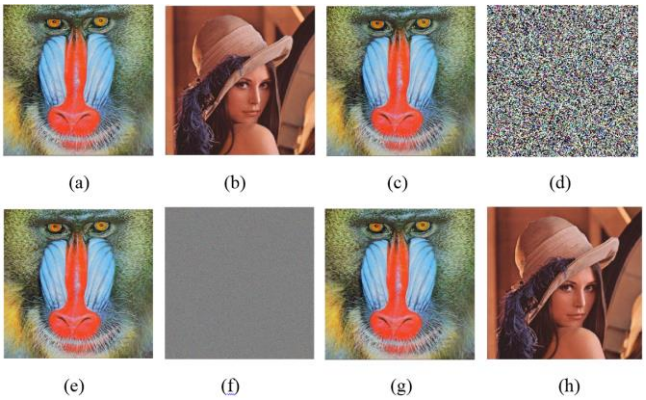

Fig. 3: a) Colour cover image 256×256, b) secret image 128×128, c) IWT applied cover image, d) chaos encryption with chaotic tent map applied secret image, e) embedded image, f) AES encrypted image, g) decrypted cover image, h) decrypted secret image

The performance analysis of proposed encryption algorithm: hybrid image encryption for colour images (Lena and baboon) is demonstrated in the table 1. Here, the performance evaluation is done in three ways; normal colour image, with crop attacks (25% and 50%), and with noise attacks (25% of SP noise and 25% of Gaussian noise). The proposed encryption algorithm delivers 50.90 dB of PSNR, 7.33 of entropy value and 33.46% of UACI for normal colour image (Lena). Respectively, the proposed encryption algorithm delivers 34.80 dB of PSNR, 7.44 of entropy value and 33.45% of UACI for normal colour image (baboon). Subsequently, the proposed encryption algorithm achieved better results in the circumstances of noise attacks and crop attacks by means of entropy value, PSNR, and UACI.

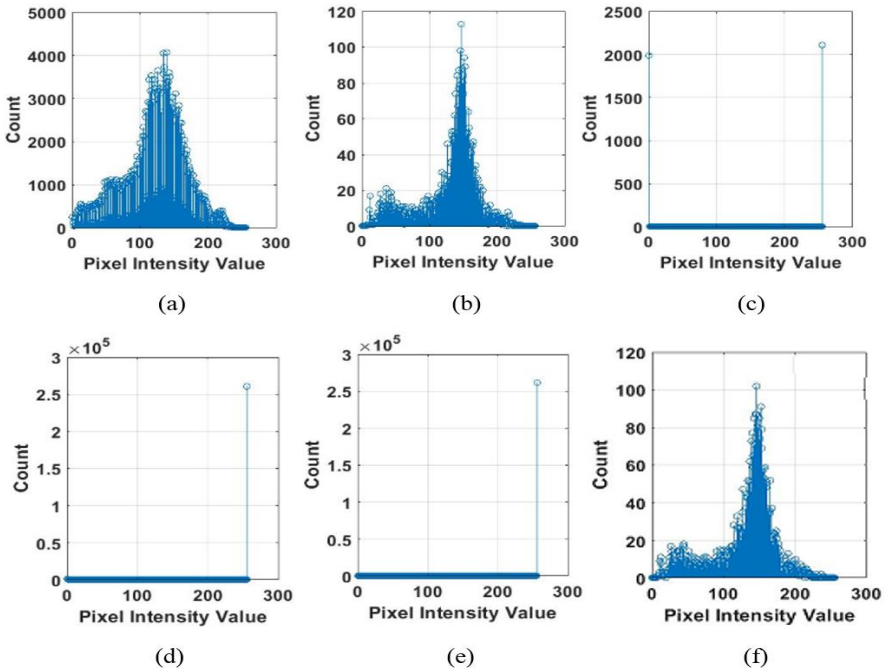

Fig. 4: Histogram diagram of colour image a) Cover image b) secret image c) chaos encryption with chaotic tent map image d) AES encrypted image e) AES decrypted image f) chaos decryption with chaotic tent map image

Table 1. Performance analysis of colour image by means of entropy value, PSNR, and UACI

Proposed algorithm	**Colour Images**	**Performance measure**	**Normal**	**Crop attacks**		**Noise attacks**	
						SP noise	**Gaussian**
				25%	50%	25%	25%
Hybrid image encryption	Lena	PSNR (dB)	50.90	23.11	19.65	18.79	11.25
		Entropy	7.33	6.98	6.67	6.93	5.25
		UACI (%)	33.46	33.43	33.56	33.47	33.45
	Baboon	PSNR (dB)	34.80	23.01	19.75	17.28	13.79
		Entropy	7.44	6.88	6.05	6.91	6.99
		UACI (%)	33.45	33.42	33.43	33.45	33.42

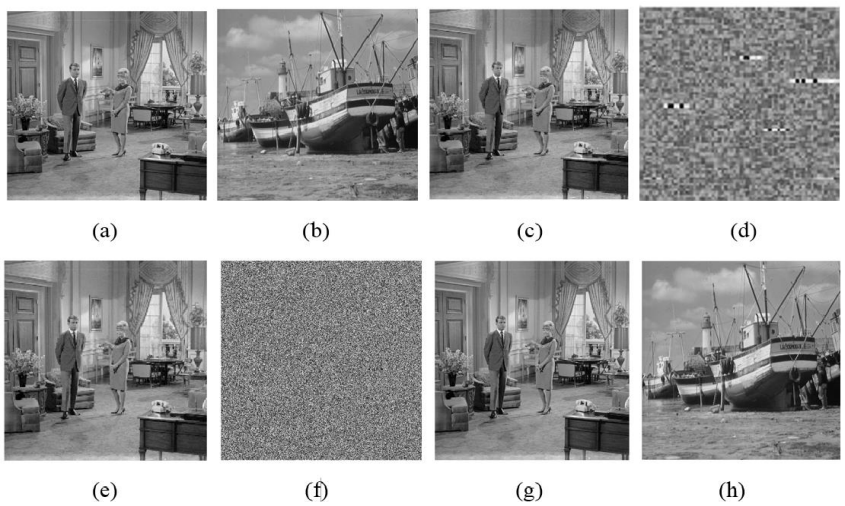

Fig. 5: a) Grayscale cover image 256×256 , b) secret image 128×128 , c) IWT applied cover image, d) chaos encryption with chaotic tent map applied secret image, e) embedded image, f) AES encrypted image, g) decrypted cover image, h) decrypted secret image

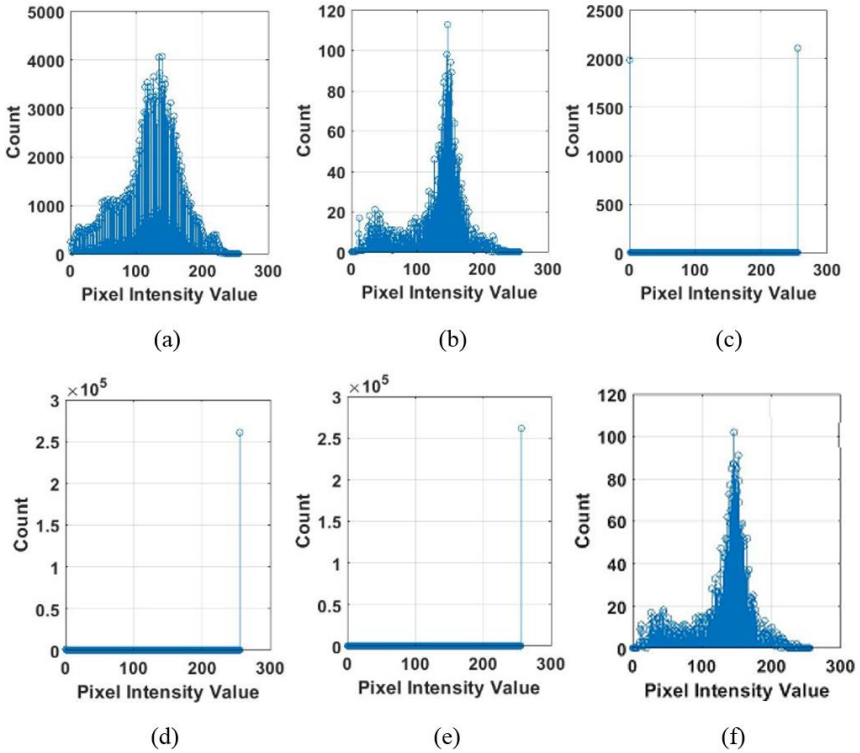

Fig. 6: Histogram diagram of grayscale image a) Cover image b) secret image c) chaos encryption with chaotic tent map image d) AES encrypted image e) AES decrypted image f) chaos decryption with chaotic tent map image

C. Quantitative analysis on grayscale images

In this sub-section, Fig. 5 denotes the grayscale images (Boat and couple), which are undertaken for image embedding and extracting process. Figure 5(a) represents grayscale cover image (couple) and Fig. 5(b) indicates secret image (boat). The image after applying IWT in grayscale cover image is indicated in the Fig. 5(c). Similarly, the image after applying chaos encryption with chaotic tent map in secret image is showed in the Fig. 5(d). The embedded encrypted secret image and transformed colour image is denoted in the Fig. 5(e). Fig. 5(f) denotes the encrypted image after performing AES encryption algorithm in the embedded image. Finally, the decrypted colour and secret images are given in the Fig. 5(g) and 5(h). Consequently, the histogram representation of grayscale image is specified in the Fig. 6.

Table 2 demonstrates the performance analysis of proposed encryption algorithm for grayscale images (boat and couple) in three different circumstances; normal colour image, with crop attacks (25% and 50%), and with noise attacks (25% of SP noise and 25% of Gaussian noise). The proposed encryption algorithm achieved 39.17 dB of PSNR, 7.34 of entropy value and 39.24% of UACI for normal grayscale image (boat). Correspondingly, the proposed encryption algorithm achieved 38.17 dB of PSNR, 7.24 of entropy value and 39.17% of UACI for normal grayscale image (couple). Similarly, the proposed encryption algorithm delivered superior results in the circumstances of noise attacks and crop attacks by means of entropy value, PSNR, and UACI.

Table 2. Performance analysis of grayscale image by means of entropy value, PSNR, and UACI

Proposed algorithm	**Grayscale Images**	**Performance measure**	**Normal**	**Crop attacks**		**Noise attacks**	
						SP noise	**Gaussian**
				25%	50%	25%	25%
Hybrid image encryption	Boat	PSNR (dB)	39.17	24.79	20.23	19.23	12.46
		Entropy	7.34	6.97	7.01	6.77	6.66
		UACI (%)	39.24	38.67	37.45	38.19	38.03
	Couple	PSNR (dB)	38.17	19.72	17.17	18.44	13.95
		Entropy	7.24	6.82	6.78	6.47	6.23
		UACI (%)	39.17	38.97	38.61	39.09	39.02

D. Comparative analysis

The comparative analysis of proposed and existing works is described in the table 3. S. Roy, and A.K. Pal, [16] decomposed the blue and green components from the cover image. Then, two dimensional Discrete Cosine Transform (DCT) was applied to every block of the blue and green components. Here, a binary watermark

bit was embedded in the transformed blocks of green and blue components in order to ensure the imperceptibility of the watermarked cover image. The performance of developed methodology was evaluated in the circumstances like deletion of columns/lines, cropping, rotation, scaling, noise addition, low pass filtering attacks, gamma correction, and histogram equalization attacks. In this research paper, the developed methodology achieved 42.2198 dB of PSNR value for a colour image (Lena).

In addition, M. Zarebnia, et al. [17] developed an effective and fast multiple image encryption algorithm on the basis of chaotic

system. Here, a combination of chaotic maps (logistic map, tent map, two dimensional Arnold cat map, and sine map) were used to create pseudorandom sequences for replacing the sub-blocks of a plain image. These sub-blocks were combined by employing chaos sequences that were generated with the combination of chaotic systems. Experimental analysis and simulation outcomes showed that the developed algorithm resists against the dissimilar attacks effectively and strongly. The developed encryption method achieved 7.1905 of entropy value and 33.4274% of UACI value for a grayscale image (boat). Additionally, the developed methodology was tested with different circumstances like noise and crop attacks. Compared to the existing works, the proposed encryption algorithm achieved a superior performance in terms of entropy value, PSNR, and UACI. The proposed hybrid encryption is mathematically efficient and also it is suitable for numerous key lengths.

Table 3. Comparative analysis of proposed and existing approaches

Methods	**Images**		**PSNR (dB)**	**Entropy**	**UACI (%)**
DCT based encryption [16]	Colour image (Lena)	Normal	42.2198	-	-
Fast multiple image encryption algorithm [17]	Grayscale image (Boat)	Normal	-	7.1905	33.4274
		25% crop	15.3363	-	-
		50% crop	12.2980	-	-
		25% SP noise	15.2425	-	-
		25% Gaussian noise	10.5678	-	-
Hybrid image encryption	Colour image (Lean)	Normal	50.90	7.33	33.46
		25% crop	23.11	6.98	33.43
		50% crop	19.65	6.67	33.56
		25% SP noise	18.79	6.93	33.47
		25% Gaussian noise	11.25	5.25	33.45
	Grayscale image (Boat)	Normal	39.17	7.34	39.24
		25% crop	24.79	6.97	38.67
		50% crop	20.23	7.01	37.45
		25% SP noise	19.23	6.77	38.19
		25% Gaussian noise	12.46	6.66	38.03

V. CONCLUSION

This research mainly focused on developing a highly secured transmission network for real time applications. Initially, the low frequency IWT was applied in the cover image for perfect reconstruction of the original image. Then, chaos encryption with chaotic tent map was used with the combination of AES (128 bit) encryption for ensuring the privacy and integrity of data in the secret image. For embedding the secret image in cover image, a simple methodology: LSB was applied that alters the bit value of cover image for hiding the secret image. After embedding process, extracting process was performed by using chaos decryption with chaotic tent map and AES (128 bit) decryption method for retrieving the original secret image from the cover image. The proposed hybrid encryption algorithm performance was evaluated by applying the performance measures like PSNR and entropy value, and UACI. Compared to other existing encryption algorithms, the proposed algorithm almost achieved 2-9 dB enhancement in PSNR, 0.15 improvement in entropy value, and 6.2% improvement in UACI value. In future work, a superior image encryption algorithm can be developed for further improving the efficiency and effectiveness of the image cryptography.

REFERENCES

[1] Wang XY & Li ZM (2019), A colour image encryption algorithm based on Hopfield chaotic neural network. Optics and Lasers in Engineering, 115, 107-118.

[2] Li CL, Li HM, Li FD, Wei DQ, Yang XB, & Zhang J (2018), Multiple-image encryption by using robust chaotic map in wavelet transform domain. Optik, 171, 277-286.

[3] Dhall S, Pal SK, & Sharma K (2018), Cryptanalysis of image encryption scheme based on a new 1D chaotic system. Signal Processing, 146, 22-32.

[4] Ye G, & Huang X (2017), An efficient symmetric image encryption algorithm based on an intertwining logistic map. Neurocomputing, 251, 45-53.

[5] Chen J, Zhang Y, Qi L, Fu C, & Xu L (2018), Exploiting chaos-based compressed sensing and cryptographic algorithm for image

[6] encryption and compression. Optics & Laser Technology, 99, 238-248.

[7] Wu J, Xie Z, Liu Z, Liu W, Zhang Y, & Liu S(2016), Multiple-image encryption based on computational ghost imaging. Optics Communications, 359, 38-43.

[8] Lahdir M, Hamiche H, Kassim S, Tahanout M, Kemih K, & Addouche SA, A novel robust compression-encryption of images based on SPIHT coding and fractional-order discrete-time chaotic system. Optics & Laser Technology, 109, 534-546.

[9] Halagowda SRM, & Lakshminarayana SK (2017), Image Encryption Method based on Hybrid Fractal-Chaos Algorithm. International Journal of Intelligent Engineering and Systems, 10, 221-229.

[10] Ratnavelu K, Kalpana M Balasubramaniam P, Wong K, & Raveendran P (2017), Image encryption method based on chaotic fuzzy cellular neural networks. Signal Processing, 140, 87-96.

[11] Essaid M. Akharraz I, Saaidi A, & Mouhib A (2018), A New Image Encryption Scheme Based on Confusion-Diffusion Using an Enhanced Skew Tent Map. Procedia Computer Science, 127, 539-548.

[12] Wang X, Zhu X, Wu X, & Zhang, Y (2018), Image encryption algorithm based on multiple mixed hash functions and cyclic shift. Optics and Lasers in Engineering, 107, 370-379.

[13] Daneshgar A, & Khadem B (2015), A self-synchronized chaotic image encryption scheme. Signal Processing: Image Communication, 36, 106-114.

[14] Pak C, & Huang L (2017). A new colour image encryption using combination of the 1D chaotic map. Signal Processing, 138, 129-137.

[15] Zhang X, Meng X, Wang Y, Yang X, Yen Y, Li X, Peng X, He W, Dong G, & Chen H (2018), Hierarchical multiple-image encryption based on the cascaded interference structure and vector stochastic decomposition algorithm. Optics and Lasers in Engineering, 107, 258-264.

[16] Li H, Wang Y, & Zuo Z (2019), Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms. Optics and Lasers in Engineering, 115, 197-207.

[17] Roy S, & Pal AK (2017), A blind DCT based colour watermarking algorithm for embedding multiple watermarks. AEU-International Journal of Electronics and Communications, 72, 149-161.

[18] Zarebnia M, Pakmanesh H, & Parvaz R (2019), A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images. Optik, 179, 761-773.

T. Venugopal presently working as a Director in Anubose Institute of Technology, Paloncha, Telangana with around 28 years of experience in teaching field. Member of PIC, PRC of DTDDF Center of BARC at ABIT and coordinator for the BARC's DAE Technology's Display and Dissemination Facility Center. Field of interest is in digital image processing. Guided number of Projects for UG and PG students. Life member of Institute of Engineers, IETE & ISTE.

Dr. V. Siva Kumar Reddy presently working as a Principal, in MRCET, Hyderabad with a 22 years of experience in teaching field. Doctorate from IIT Kharagpoor and his Masters in Engineering is from JNTU Hyderabad. Computer Networks and Communications, Video and Signal processing are his main interests of research. He published around 110 National and International journals and guided many Ph.D Scholors. Also a reviewer for many National and International Journals.