Received: July 9, 2021. Revised: September 15, 2021.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Image Watermarking Based on Chaos Encryption with Hybrid Mapping and Grey Wolf Optimizer

Sharon Rose Victor Juvvanapudi[1]* **Pullakura Rajesh Kumar[1]** **Konala Veera Venkata Satyanarayana Reddy[1]**

[1]*Electronics and communication Engineering Department, Andhra university, Visakhapatnam, India*
* Corresponding author's Email: jsr.victor@gmail.com

Abstract: In this study, a new watermarking system was proposed to address two major concerns: slow learning and computational capability. At first, cover image was transformed into wavelet environment utilizing Integer Wavelet Transform (IWT) that makes the cover image free from false errors. Then, Grey Wolf Optimizer (GWO) was utilized for selecting the image pixels to embed the secret image in the cover image. GWO effectively selects the pixels utilizing fitness function, which calculates entropy, pixel intensity and edge of the cover images. Besides, the secret image was encrypted by using chaos encryption with hybrid mapping (logistic and henon map) that improves computation efficiency and security with good embedding capacity. After the cover image transformation and secret image encryption, Least Significant Bit (LSB) was utilized to deliver self-recovery features and also for locating the tempered region in the digital image. Experimental results showed that the developed system attained a secure transmission network with low complexity in light of Unified Averaged Changed Intensity (UACI), entropy value, Structural Similarity Index (SSIM), Normalized Cross Correlation (NCC), and Peak Signal-to-Noise Ratio (PSNR). Compared to the existing systems, the proposed system showed 3dB to 4.4 dB improvement in PSNR and 0.32 value improvement in SSIM.

Keywords: Chaos encryption with hybrid mapping, Grey wolf optimizer, Integer wavelet transform, Least significant bit.

1. Introduction

In recent periods, the rapid growth of internet and information technology has made the capture, propagation and storage of the multimedia data such as image, video, and audio are extremely convenient and also it is suitable to access digital devices and images [1, 2]. Besides, a new set of issues related to security are arisen such as manipulation, unrestricted distribution, and duplication of multimedia [3]. In order to address these issues, watermarking is considered as an effective technique. Digital image watermarking is a mechanism of embedding secrete image in the cover image that effectively improves the system security [4-6]. The watermarking techniques are utilized for several purpose that includes data integrity, content authentication, individual identification, and copy control [7, 8]. Currently, numerous methods are developed in image watermarking like interval type-2 fuzzy logic system [9], artificial bee colony [10], singular value decomposition [11], Arnold transform with back propagation neural network [12], discrete cosine transform [13], double random phase encoding [14], etc. Though, the above mentioned methodologies achieved good performance, still the developed systems are not proven reliable for image watermarking, due to some image factors such as illumination, lighting variations, etc. So, the important goal of the present research work is to develop an efficient system in order to overcome the current demerits to present a secure data transmission.

In this research, a new watermarking system is proposed for secure data transmission with low computational complexity. In image watermarking, two types of images (cover and secret image) were used for experimental study, for instance, Lena, Pepper, Monalisa, Baboon, Barbara, etc. Before embedding the secret image in the cover image, chaos encryption with hybrid mapping (logistic map and henon map) was employed in the secrete image. The chaos encryption with hybrid mapping effectively prevents the loss of information and also delivers a good data safety assurance with low computational complexity that was eligible to enhance the efficiency and security of transmission. Similarly, an appropriate transformation (IWT) was applied in the cover image with GWO. Related to other wavelet transforms, IWT effectively decreases the data loss in the extracted secrete and cover images. In addition, GWO effectively selects the image pixels for embedding the secret image in the cover image. The GWO selects the pixels utilizing fitness function that calculates entropy, pixel intensity and edge of the cover images. In addition, chaos encryption with hybrid mapping 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, decryption phase was carried-out to decrypt the cover image from the secret image. A few performance measures are undertaken for experimental investigation to verify the proposed system performance.

Section 2 surveys some research papers on image watermarking. Mathematical description about the proposed system is stated in the Section 3. In Section 4, quantitative and comparative investigation of the proposed and existing systems are detailed. In Section 5, conclusion about the present research work is detailed.

2. Literature review

Abuturab [15] developed a new wavelet transform and optical interference based image watermarking system for secure data transmission. In this research work, the information of each and every secret image was encoded into three Phase-Only Masks (POMs). In that, one POMs denotes user identity key and the remaining two POMs were stated as user identity key, which were modulated by utilizing gyrator transform domain. The experimental consequence of the developed system guarantees that the final decrypted image was exactly similar as the original secret image. The developed system performance was degraded, if the key bit size was high in the extracting procedure. Wang [16] presented a new watermarking system (Singular Value Decomposition Ghost Imaging (SVDGI)) for secure data transmission. Initially, encrypt the watermark image using (SVDGI) and then embed the encrypted watermark image in the host image utilizing lifting wavelet transform and discrete cosine transform. Henceforth, the developed system has good imperceptibility, robustness and large capacity, while extracting the watermark image from the host image. Experimental outcome showed that the developed system attained better security level with low computational complexity. In this work, the decrypted watermark image should be equal to the host image, orelse the computational complexity of the system will be high.

Shao [17] presented a robust watermarking system using chaotic map and Orthogonal Fourier Mellin Moments (OFMM). The developed system comprises of two main phases such as verification phase and registration phase. At first, two images were combined in a single channel design and then the feature invariants were derived by utilizing OFMM for constructing a binary feature image. Besides, chaotic map was used to generate the verification image. Compared to other systems, the developed system effectively saves the storage space and attains high level security. Experimental outcome exhibits the security performance and efficiency of the developed watermarking system. In contrast, the developed system performed poorly in encrypting the digital images with the homogeneous background. Amiri [18] developed a new human vision system on the basis of spread spectrum method for scalable image watermarking. At every wavelet sub-band, the watermark image was embedded in the selected sub-band coefficients. Therefore, these coefficients were selected by independent analysis of contrast, luminance information and texture in the low frequency sub-band of wavelet transform. Besides, the coefficient selection was done utilizing local entropy and coefficients amplitude in the high frequency sub-band of wavelet transform. Experimental section showed that the developed image watermarking system attained better security and also resist dissimilar attacks. The developed system failed to achieve better results in image watermarking, due to poor contrast of the reconstructed cover image.

Ghadi [19] developed a blind spatial domain based image watermarking system, which utilizes association rule mining techniques and texture analysis. In this research study, a few gray scale histogram based image features (entropy, DC coefficients, skewness, and kurtosis) were used to select the input data for designing association rules. Successively, Apriori approach was used for mining the interactions between the selected features. Finally, association rule mining computes two parameters (confidence and lift) for designing the blind watermarking. The developed method needed much improvement in constructive and unifying framework in order to handle noise attacks with more images. Setyono and Setiadi [20] developed a novel image encryption algorithm that combines singular value decomposition and Tchebichef. In addition, an Arnold's algorithm was used for enhancing the visual quality and security of the watermarked image. In this literature study, the cover image was categorized into smaller blocks, and then transformed by Tchebichef. The extensive experiment showed that the developed model obtained better performance against numerous attacks such as signal processing, geometry, filtering, and noise addition. However, the developed image encryption algorithm showed limited performance under homogeneous background.

Setyono and Setiadi [21] introduced a new robust watermarking algorithm which combines Tchebichef transform, and singular value decomposition. In this literature study, embedding was done on the selected frames for maintaining the imperceptibility. Here, the frame selection was processed by linear congruential generator and the selected frames were transformed into color space from RGB to YCbCr. The developed watermarking algorithm failed in achieving effective decryption results in terms of error rate. Venugopal and Reddy [22] used a multi-purpose watermarking algorithm for robust image encryption. At first, the cover image was transformed into wavelet domain by IWT algorithm and then chaotic logistic mapping was for encrypting logo image. Then, least significant bit and Rivest–Shamir–Adleman algorithms were used to locate the tempered region in the digital image and to enhance the security with better embedding capacity and high computational efficiency. The main problem in the developed algorithm was stealth effects in the presence of message. To address the aforementioned issues, a new watermarking system is proposed in this article to enhance the security of data transmission.

3. Proposed system

With the rapid growth of network technology, the access, transmit, save and distribution of digital data (audio, video, image and text) is cost effective and low complexity. Additionally, the availability of image processing tools has made data transmission much easier to download and access the digital images. In present time, the image watermarking technique has received much attention among the researchers for protecting ones ownerships and copyrights. In this research, a new image watermarking system is proposed to further improve the security of data transmission. The proposed image watermarking system contains six steps: image collection, chaos encryption with hybrid mapping, IWT, optimization of wavelet sub-bands using GWO, LSB, and decryption phase. Work flow of the proposed image watermarking system is stated in Fig. 1, and the detailed explanation about the proposed system is described below.

3.1 Image collection

Generally, in image watermarking, two types of images (cover image and secret image) are used for experimental investigation. The cover image is utilized to embed the secret image, which should be a noiseless and appropriate. The sample collected greyscale and color digital images are graphically represented in Fig. 2.

3.2 Chaos encryption with hybrid mapping

After collecting the digital images, the secret image is encrypted using chaos encryption with hybrid mapping (logistic map and henon map). Presently, chaos encryption has extensive reputation among researchers, because of its inherent features of chaos systems. Commonly, the chaos image cryptosystem comprises of two phases; permutation and diffusion. In diffusion phase, each and every pixel values are altered by applying chaos sequences. Respectively, in the permutation phase, the pixel permutation is considered as the position of image pixels that are scrambled over the entire image without disturbing the image pixel values. In this research, the permutation and diffusion phases are performed by using the generated keys K_i and the value of logistic map and henon map. In chaos encryption, the simplest chaotic maps are henon map and logistic map, which are mathematically given in the Eq. (1) and (2). Logistic map is a polynomial mapping of degree two that exhibits chaotic behaviour.

The logistic map is mathematically given in Eq. (1).

$$l_{map} = \mu x_n (1 - x_{n-1}) \tag{1}$$

Where, x_n is represented as chaos sequence that ranges between [0, 1], and μ is represented as control parameter that ranges $\mu \in (3.57,4)$. The chaotic system exhibits better sensitivity to initial conditions, when the parameter approaches is four. Correspondingly, the henon map is a two dimensional reversible non-linear chaotic map that

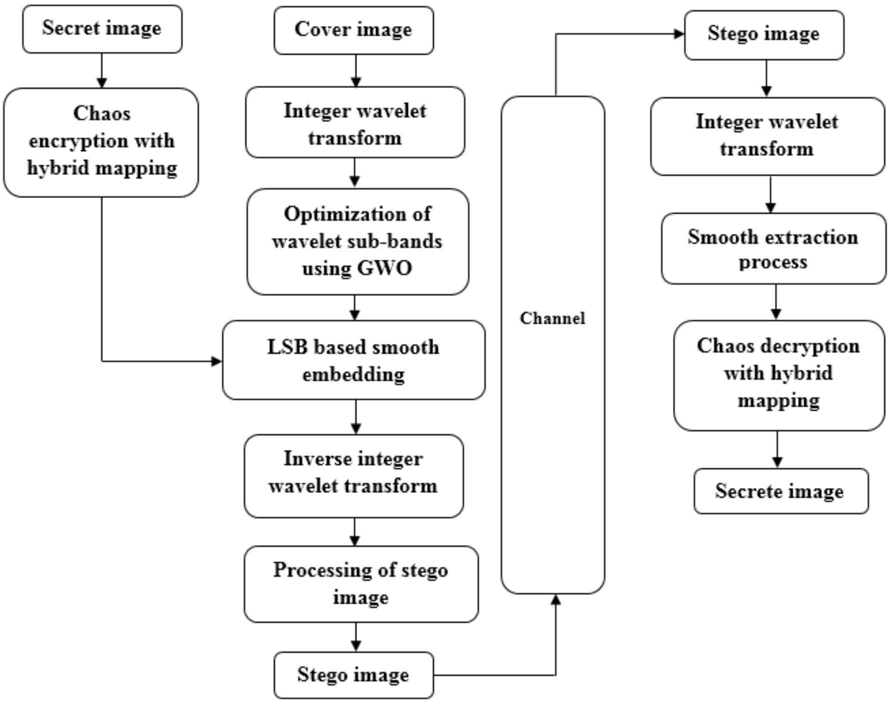
Secret image
Chaos encryption with hybrid mapping
Cover image
Integer wavelet transform
Optimization of wavelet sub-bands using GWO
LSB based smooth embedding
Inverse integer wavelet transform
Processing of stego image
Stego image
Channel
Stego image
Integer wavelet transform
Smooth extraction process
Chaos decryption with hybrid mapping
Secrete image

Figure. 1 Workflow of proposed system

Figure. 2 Sample collected digital images

iterates the point (x_n, y_n), which is mathematically denoted in Eq. (2).

$$h_{map} = 1 - ax_n^2 + y_n, \quad y_{n+1} = bx_n \tag{2}$$

Where, $a\epsilon(0,1.4)$, $b\epsilon(0.2, 0.314)$ are denoted as control parameters and the working process of henon map mainly depends on the parametric values. Besides, iterate the hybrid mapping (logistic map and henon map) for five times in order to accomplish rid of the transient effect by using the parameter value of hybrid mapping and generated keys K_i. In addition, sort the chaotic orbit which attained from the previous steps and then permutated the diffused or plain-image using Eqs. (3) and (4).

$$x_{n+1} = l_{map} + h_{map} \tag{3}$$

$$mim(i) = permut \oplus K_i(x_{n+1}\, p(i)), i = 1,2,3, \dots .p \times q \tag{4}$$

Where, p and q are represented as width and height of plain-image, $p(i)$ is indicated as original image pixel value, and $mim(i)$ is represented as image pixel value. Finally, generate the cipher key for permuted image and then diffuse the permuted image using hybrid chaotic orbit. The output of diffusion stage is cipher-image $c(i)$ that is mathematically signified in Eq. (5).

$$c(i) = mim(i)\, , i = 1,2,3, \dots p \times q \tag{5}$$

3.3 Integer wavelet transform

Similarly, the cover image is converted into transform domain utilizing IWT approach. Generally, IWT contains four level of sub-bands like High-High (HH), Low-Low (LL), High-Low (HL), and Low-High (LH). Among four available sub-bands, LL sub-band is considered, where it looks closely related to original image. The IWT coefficients are mathematically stated in the Eqs. (6) to (9).

$$LL_{i,j} = \left| \frac{(O_{2i,2j} + O_{2i+1,2j})}{2} \right| \tag{6}$$

$$HL_{i,j} = O_{2i+1,2j} - O_{2i,2j} \tag{7}$$

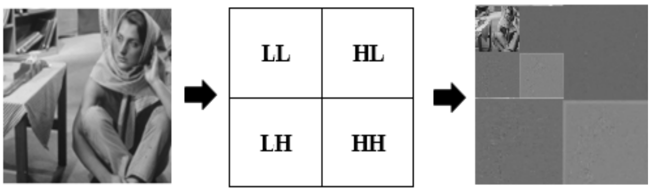

Figure. 3 Working procedure of IWT method

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

$$HH_{i,j} = O_{2i+1,2j+1} - O_{2i,2j} \quad (9)$$

Correspondingly, the coefficients of inverse-IWT are represented in the Eqs. (10) to (13).

$$O_{2i,2j} = LL_{i,j} - |\frac{HL_{i,j}}{2}| \quad (10)$$

$$O_{2i,2j+1} = LL_{i,j} + \left|(HL_{i,j+1})/2\right| \quad (11)$$

$$O_{2i+1,2j} = O_{2i,2j+1} + LH_{i,j} - L_{i,j} \quad (12)$$

$$O_{2i+1,2j+1} = O_{2i+1,2j} + HH_{i,j} - LH_{i,j} \quad (13)$$

Where, the level of each and every image pixel is represented as $(i,j), O_i$ is specified as original cover image, X is indicated as height of image pixel, Y is denoted as width of image pixel and $1 \leq i \leq \frac{X}{2}, and\ 1 \leq j \leq Y/2$ are represented as floor values. The working procedure of IWT method is graphically represented in Fig. 3.

3.4 Optimization of wavelet sub-bands using grey wolf optimizer

After cover image transformation, GWO is applied on Low-Low sub-band to select the optimal block in order to ease the embedding process. Generally, GWO is a swarm intelligence optimization method that mimics the leadership hierarchy of wolves which is known for group hunting. Usually, the grey wolfs belongs to the Canidae family, which mostly wish to live in group. The grey wolves have a strict social dominant hierarchy (leader may be a male or female) that is theoretically named as alpha (α). Mostly, the alpha is accountable for decision making and the orders of the dominant wolf follow the pack. Respectively, beta (β) represents the sub-ordinate wolves that help alpha in decision making. Beta (β) acts as an advisor to alpha and discipliner for the pack. The low ranking grey wolves are named as omega (ω) that submits all other dominant wolves. If a wolf is neither an omega or alpha nor beta, it is called delta (δ). Delta wolves dominate the omega wolves and report the status to alpha and beta wolves. The hierarchy of wolves is theoretically modelled to develop GWO and accomplish optimization. GWO algorithm is tested with the test functions that represent the exploitation and exploration characteristics compared to other swarm intelligence algorithms. Due to multipurpose property, the modified GWO algorithm attempts to solve the optimization issues.

The GWO algorithm mimics the social hierarchy and hunting behaviour of grey wolves. In addition to the hunting behaviour of grey wolves, group hunting is another appealing societal action of grey wolves. The GWO algorithm includes three main segments such as, encircling, hunting and attacking of prey. Step by step procedure of GWO algorithm is described below.

Step 1: At first, initialize the GWO parameters like design variable size Gd, search agents Gs, maximum number of iterations $iter_{max}$, and vectors a, A, C that is mathematically denoted in the Eqs. (14) and (15). The value $\vec{a}$ linearly decreases from two to zero over the course of iterations.

$$\vec{A} = 2\vec{a}.rand_1 - \vec{a} \quad (14)$$

$$\vec{C} = 2.rand_2 \quad (15)$$

Where, $rand_1$ and $rand_2$ are denoted as random vectors, which ranges between [0, 1].

Step 2: Then, randomly generate the wolves based on pack that is signified in Eq. (16).

$$Wolves = \begin{bmatrix} G_1^1 & G_2^1 & G_3^1 \ldots. & G_{Gd-1}^1 & G_{Gd}^1 \\ G_1^2 & G_2^2 & G_3^2 \ldots. & G_{Gd-1}^2 & G_{Gd}^2 \\ . & . & . \ \ldots. & . & . \\ G_1^{Gs} & G_2^{Gs} & G_3^{Gs} \ldots. & G_{Gd-1}^{Gs} & G_{Gd}^{Gs} \end{bmatrix} \quad (16)$$

Where, G_j^1 is represented as initial value of the j^{th} pack of the i^{th} wolves.

Step 3: Calculate the fitness value of each hunt agent utilizing the Eqs. (17) and (18).

$$\vec{D} = \left|\vec{C}.\vec{G}_p(t) - \vec{G}(t)\right| \quad (17)$$

$$\vec{G}(t+1) = \vec{G}_p(t) - \vec{A}.\vec{D} \quad (18)$$

Where, t is denoted as number of iteration, $\vec{A}$ and $\vec{C}$ are represented as coefficient vectors, $\vec{G}_p$ is stated as position vector of the prey, and $\vec{G}$ is stated as position vector of a grey wolf.

Step 4: Determine the best hunt agent G_α, second and third best hunt agents G_β and G_δ by using the Eqs. (19) to (24).

$$\vec{D}_\alpha = \left|\vec{C}_1 . \vec{G}_\alpha - \vec{G}\right| \tag{19}$$

$$\vec{D}_\beta = \left|\vec{C}_2 . \vec{G}_\beta - \vec{G}\right| \tag{20}$$

$$\vec{D}_\delta = \left|\vec{C}_3 . \vec{G}_\delta - \vec{G}\right| \tag{21}$$

$$\vec{G}_1 = \vec{G}_\alpha - \vec{A}_1 . (\vec{D}_\alpha) \tag{22}$$

$$\vec{G}_2 = \vec{G}_\beta - \vec{A}_2 . (\vec{D}_\beta) \tag{23}$$

$$\vec{G}_3 = \vec{G}_\delta - \vec{A}_3 . (\vec{D}_\delta) \tag{24}$$

Step 5: Update the location of the present hunt agent by utilizing Eq. (25).

$$\vec{G}\ (t+1) = \frac{\vec{G}_1 + \vec{G}_2 + \vec{G}_3}{3} \tag{25}$$

Step 6: Evaluate the fitness value of all hunts using Eq. (26).

$$Fitness = \sum_{i=1}^{n} G_i^2 \tag{26}$$

Step 7: Update the value of G_α,G_β and G_δ.

Step 8: Obtain a possible solution by using the best values of G_α,G_β and G_δ.

Step 9: Check the stopping criteria, whether the $Iteration$ reaches $Iteration_{max}$ or not, if yes, print the current best value, or else again go to step 5.

3.5 Least significant bit and decryption phase

After secrete image encryption and cover image transformation, embedding process is carried-out to hide the secrete image in the cover image. In embedding process, LSB is used as the bit position of the integer unit values. In this scenario, the pixel values of secrete and cover images are transformed into binary values by employing eight bit LSB. In this research, the secrete image size is represented as $m \times n/8$, and the cover image size is denoted as $m \times n$. In eight bit LSB, the cover image bit value is interchanged with secrete image bit value. By this way, the secrete image is embedded in the cover image. Then, the binary values are transformed into decimal numbers. In addition, inverse IWT is carried-out on the decimal numbers and the output image is named as stego image.

On the receiver side, IWT and LSB are performed on the stego image along with chaos decryption with hybrid mapping. Here, chaos decryption with hybrid mapping is performed by using the generated cipher key. At last, the secrete image is extracted with limited or no loss of information. Hence, the extracted secret image is the exact copy of the original secret image.

4. Experimental discussion

For experimental simulation, MATLAB (2018a) environment was utilized in this study with 8 GB RAM, i9 3.0 GHz processor, and 3 TB memory. The proposed system performance was related with other existing systems to validate the efficacy of the proposed watermarking system. In addition, the performance valuation of the proposed watermarking system was also done under the circumstance of noise attacks (Salt and Pepper (SP) noise and Gaussian noise), crop attacks and histogram equalization. The proposed watermarking system performance was validated in light of SSIM, entropy value, PSNR, NCC and UACI. In this research, the secret image size is fixed as 64×64, and the cover image size is fixed as 512×512. Mathematical equations of entropy value, PSNR, UACI, SSIM and NCC were indicated in the Eqs. (27) to (32).

$$E(m) = \sum_{x=0}^{m-1} p(m_x) log_2 \frac{1}{p(m_x)} \tag{27}$$

Where, $p(m_x)$ was represented as probability of symbol occurrence m_x and m was signified as total number of symbols $m_x \epsilon m$.

$$PSNR = 10\ log_{10}(\frac{255^2}{MSE}) \tag{28}$$

$$MSE = 1/pq \sum_{x=0}^{p-1} \sum_{y=0}^{q-1} [I(x,y) - k(x,y)]^2 \tag{29}$$

Where, $p\ and\ q$ were stated as row and column of the image, $k(x,y)$ was stated as decrypted image, and $I(x,y)$ was indicated as original input image.

$$UACI = \frac{1}{pq} \sum_{x=1}^{p} \sum_{y=1}^{q} \frac{|E_1(x,y) - E_2(x,y)|}{255} \times 100 \tag{30}$$

$$SSIM(x,y) = \frac{(2\mu_x \mu_y + c_1)(2\sigma_{xy} + c2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{31}$$

$$NCC = \left[\frac{\sum_{x=1}^{p} \sum_{y=1}^{q} [I(x,y) k(x,y)]}{\sum_{x=1}^{p} \sum_{y=1}^{q} [I(x,y)]^2}\right] \tag{32}$$

Received: July 9, 2021. Revised: September 15, 2021.

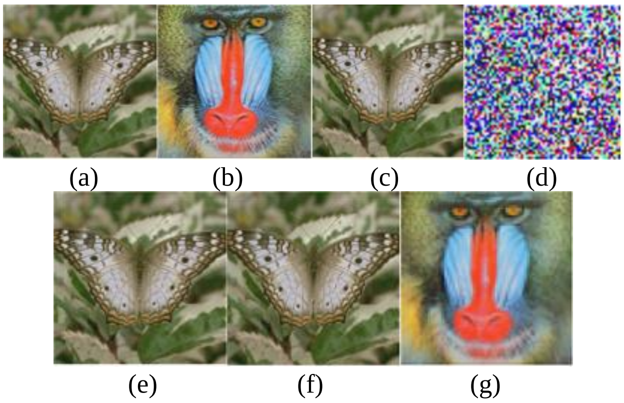

Figure. 4: (a) cover image 512×512, (b) secret image 64×64, (c) IWT applied cover image, (d) encrypted secret image, (e) embedded image, (f) decrypted cover image, and (g) decrypted secret image

Where, $x\ and\ y$ were stated as windows of filter image k and original image I,$\sigma\ and\ \mu$ were denoted as standard deviation and mean of x and y, $c_1\ and\ c_2$ were indicated as constants, and $E_1\ and\ E_2$ are indicated as encrypted image.

4.1 Quantitative investigation on color image

The experimental investigation of color image is demonstrated in this sub-section. Here, Fig. 4 represents the color images (butterfly and baboon), which are undertaken for image embedding and extracting procedure. Fig. 4(a) represents cover image (butterfly) and Fig. 4(b) states secret image (baboon). The image after employing IWT in the cover image is stated in Fig. 4(c). Similarly, the image after applying chaos encryption with hybrid mapping in the secret image is illustrated in Fig. 4(d). Embedded transformed cover image and the encrypted secret image is denoted in Fig. 4(e). The final decrypted cover and secret images are shown in the Fig. 4(f) and 4(g).

Table 1 describes about the performance analysis of the proposed watermarking system for the color images. Here, the performance valuation is carried-out in four conditions like normal color image, with noise attacks (5% of SP noise and 5% of Gaussian noise), with crop attacks (10% and 20%), and histogram equalization. The proposed watermarking system achieves 52.11 dB of PSNR, 5.532 of entropy value, 0.999 of SSIM, 33.46% of UACI, and 0.999 of NCC for the normal color image (Butterfly as a cover image). Similarly, the proposed watermarking system delivers 99 dB of PSNR, 7.51 of entropy value, 33.46% of UACI, and 1 of NCC and SSIM for the normal color image (Baboon as a secrete image). Successively, the proposed watermarking system attained better results in the conditions; histogram equalization, noise attacks and crop attacks by means of entropy value, PSNR, SSIM, UACI and NCC.

4.2 Quantitative investigation on grayscale image

In this sub-section, Fig. 5 indicates the grayscale images (Lena and cameraman), which are used for image watermarking process. Fig. 5(a) states grayscale cover image (Lena) and Fig. 5(b) represents secret image (cameraman). The image after applying IWT in grayscale cover image is stated in Fig. 5(c). Similarly, the image after applying chaos encryption with hybrid mapping in a secret image is indicated in Fig.5 (d). The embedded encrypted secret image and transformed greyscale image is signified in Fig. 5(e). Finally, the decrypted cover and secret images are stated in the Fig. 5(f) and 5(g).

Table 2 states the performance analysis of proposed watermarking system for grayscale images in four different conditions; normal grayscale image, histogram equalization, with crop attacks (10% and 20%), and with noise attacks (5% of SP and Gaussian noise). The proposed watermarking system achieved 53.02 dB of PSNR, 7.44 of entropy value, 0.99 of SSIM, 0.99 of NCC, and 33.46% of UACI

Table 1. Performance analysis of color image by means of entropy value, PSNR, UACI, SSIM, and NCC

Color Images	Performance measure	Normal	Histogram equalization	Crop attacks		Noise attacks	
						SP noise	Gaussian
				10%	20%	5%	5%
Butterfly as cover image	PSNR (dB)	52.11	52.15	52.1	52.15	52.085	52.264
	SSIM	0.999	0.999	0.999	0.999	0.999	0.999
	NCC	0.999	0.999	0.999	0.999	0.999	0.999
	Entropy	5.532	5.532	5.532	5.532	5.532	5.532
	UACI (%)	33.46	33.46	33.46	33.46	33.46	33.46
Baboon as secret image	PSNR (dB)	99	23.473	28.04	21.10	36.061	26.07
	SSIM	1	0.938	0.986	0.951	0.989	0.987
	NCC	1	0.998	0.993	0.963	0.997	0.998
	Entropy	7.51	7.885	7.524	7.481	7.458	7.480
	UACI (%)	36.46	33.46	33.46	33.46	33.46	33.46

Received: July 9, 2021. Revised: September 15, 2021.

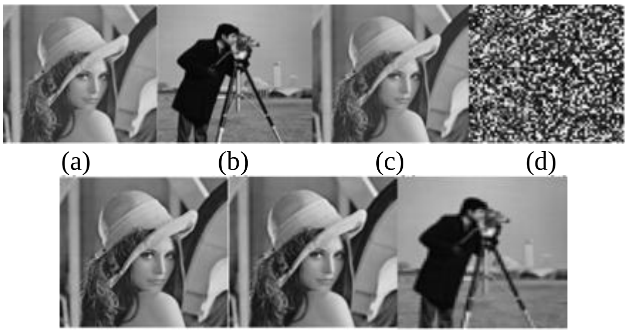

Figure. 5: (a) grayscale cover image 512 × 512, (b) secret image 64 × 64, (c) IWT applied cover image, (d) encrypted secret image, (e) embedded image, (f) decrypted cover image, and (g) decrypted secret image

for the normal grayscale image (Lena as cover image). Similarly, the proposed watermarking system attained 99 dB of PSNR, 1 of SSIM, 7.05 of entropy value, 33.46% of UACI, and 1 of NCC for the normal grayscale image (Cameraman as cover image). Correspondingly, the proposed watermarking system delivers superior results in the conditions of noise attacks, histogram equalization and crop attacks by means of SSIM, PSNR, UACI, NCC, and entropy value.

4.3 Comparative study

The comparative analysis of proposed and the existing works are described in the Tables 3 and 4. M. Ghadi [19] presented a blind spatial domain based image watermarking system using association rule mining and texture analysis. The aim of this research paper was to find effective texture locations in the host image to insert the watermark image. The experimental result showed that the developed system attained robust embedding rate with low execution time. The developed watermarking system achieved 49.17dB, 48.6dB, 48.67dB, and 50dB of PSNR for greyscale images (Lena, Baboon, Boat, and Barbara). Setyono and Setiadi [20] introduced a new image encryption algorithm based on Tchebichef and singular value decomposition technique. In addition, Arnold algorithm was used to improve the security, and visual quality of the watermarked images. The extensive experiments showed that the developed algorithm obtained 45.60dB, and 45.22dB of PSNR value for baboon, and Lena images. Related to these existing papers, the proposed watermarking system achieved more PSNR value of 53.02dB for Lena, 52.96dB for Baboon, 53.02dB for Boat, and 53.03dB for Barbara.

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

Gray scale Images	**Performance measure**	**Normal**	**Histogram equalization**	**Crop attacks**		**Noise attacks**	
						SP noise	**Gaussian**
				10%	**5%**	**5%**	**5%**
Lena as cover image	PSNR (dB)	53.02	52.28	53.02	52.94	53.08	53.08
	SSIM	0.99	0.99	0.99	0.995	0.995	0.995
	NCC	0.99	0.99	0.99	0.999	0.999	0.999
	Entropy	7.44	7.44	7.44	7.445	7.445	7.445
	UACI (%)	33.46	33.46	33.46	33.46	33.46	33.46
Cameraman as secret image	PSNR (dB)	99	19.76	24.68	31.234	25.211	25.211
	SSIM	1	0.78	0.97	0.664	0.684	0.684
	NCC	1	0.94	0.96	0.993	0.996	0.996
	Entropy	7.05	7.87	7.07	7.207	7.196	7.196
	UACI (%)	33.46	33.46	33.46	33.463	33.463	33.463

Table 3. Comparative investigation in terms of PSNR value

Methods	**Images**	**PSNR (dB)**
Blind spatial domain-based image watermarking system [19]	Lena as greyscale cover image	49.17
	Baboon as greyscale cover image	48.6
	Boat as greyscale cover image	48.67
	Barbara as a greyscale cover image	50
Tchebichef and singular value decomposition technique [20]	Baboon as greyscale cover image	45.60
	Lena as greyscale cover image	45.22
Proposed image watermarking system	**Lena as greyscale cover image**	**53.02**
	Baboon as greyscale cover image	**52.96**
	Boat as greyscale cover image	**53.02**
	Barbara as a greyscale cover image	**53.03**

Table 4. Comparative investigation in terms of PSNR and SSIM value

Methods	Images	PSNR (dB)	SSIM
IWT-Rivest–Shamir–Adleman algorithm [22]	**Lena as greyscale cover image**	36.25	0.67
Proposed image watermarking system		**53.02**	**0.99**

Venugopal and Reddy [22] developed a new multi-purpose watermarking algorithm on the basis of IWT and Rivest–Shamir–Adleman algorithm for effective image encryption. The experimental results showed that the developed algorithm attained 36.25dB PSNR value, and 0.67 SSIM value for Lena image. Hence, the proposed image watermarking system obtained effective results compared to the existing algorithm, which is depicted in Table 4.

Compared to the existing algorithms, the proposed system effectively avoids the loss of information and obtained better data safety assurance with minimum computational complexity that highly enhances the efficiency, and security of transmission, even under the conditions of homogeneous background. Further, identifying the optimal set of multiple scaling factor is a complex problem in image watermarking which is effectively solved by a multi-objective optimizer (GWO). As seen in the quantitative analysis section, the proposed image watermarking system effectively overcomes the concerns mentioned in the literatures [16-21].

5. Conclusion

The aim of this research study is to propose a highly secured transmission network for real-time applications. Initially, IWT and GWO are applied in the cover image for perfect reconstruction of original digital image. In addition, chaos encryption with hybrid mapping is implemented to ensure the privacy and integrity of data in the secret image. For embedding the secret image in the cover image, LSB is employed that alters the bit value of the cover image to hide the secret image. After embedding, the extraction procedure is carried-out utilizing IWT and chaos decryption with hybrid mapping for retrieving original secret image from the cover image. The proposed system performance is evaluated by utilizing the performance measures: PSNR, SSIM, entropy value, UACI, and NCC. Compared to the existing systems, the proposed image watermarking system showed 3 dB to 4.4 dB enhancement in PSNR value, and 0.32 value improvement in SSIM on the multimedia images; Baboon, Boat, Barbara and Lena. As a future extension, a new optimization algorithm is combined with chaos encryption to further enhance the image watermarking performance.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper background work, conceptualization, methodology have been done by 3rd Author. Dataset collection, implementation, result analysis and comparison, preparing and editing draft, visualization have been done by first author. The supervision, review of work and project administration, have been done by second author.

References

[1] J. Abraham and V. Paul, "An imperceptible spatial domain colour image watermarking scheme", *Journal of King Saud University-Computer and Information Sciences*, Vol. 31, No. 1, pp. 125-133, 2019.

[2] Y. Zhang and Y. Sun, "An image watermarking method based on visual saliency and contourlet transform", *Optik*, Vol. 186, pp. 379-389, 2019.

[3] A. Fatahbeygi and F. A. Tab, "A highly robust and secure image watermarking based on classification and visual cryptography", *Journal of Information Security and Applications*, Vol. 45, pp. 71-78, 2019.

[4] M. Moosazadeh and G. Ekbatanifard, "A new DCT-based robust image watermarking method using teaching-learning-Based optimization", *Journal of Information Security and Applications*, Vol. 47, pp. 28-38, 2019.

[5] H. Xu, X. Kang, Y. Chen, and Y. Wang, "Rotation and scale invariant image watermarking based on polar harmonic transforms", *Optik*, Vol. 183, pp. 401-414, 2019.

[6] T. H. The, C. H. Hua, N. A. Tu, T. Hur, J. Bang, D. Kim, M. B. Amin, B. H. Kang, H. Seung, and S. Lee, "Selective bit embedding scheme for robust blind colour image watermarking", *Information Sciences*, Vol. 426, pp. 1-18, 2018.

[7] A. M. Abdelhakim and M. Abdelhakim, "A time-efficient optimization for robust image watermarking using machine learning", *Expert Systems with Applications*, Vol. 100, pp. 197-210, 2018.

[8] S. Kumar, N. Jain, and S. L. Fernandes, "Rough set based effective technique of image watermarking", *Journal of Computational Science*, Vol. 19, pp. 121-137, 2017.

[9] A. Abbasi, C. S. Woo, and S. Shamshirband, "Robust image watermarking based on Riesz transformation and IT2FLS", *Measurement*, Vol. 74, pp. 116-129, 2015.

[10] F. Y. Bakhsh, and M. E. Moghaddam, "A robust HDR images watermarking method using artificial bee colony algorithm", *Journal of Information Security and Applications*, Vol. 41, pp. 12-27, 2018.

[11] C. Patvardhan, P. Kumar, and C. V. Lakshmi, "Effective colour image watermarking scheme using YCbCr colour space and QR code", *Multimedia Tools and Applications*, Vol. 77, No. 10, pp. 12655-12677, 2018.

[12] L. Sun, J. Xu, S. Liu, S. Zhang, Y. Li, and C. A. Shen, "A robust image watermarking scheme using Arnold transform and BP neural network", *Neural Computing and Applications*, Vol. 30, No. 8, pp. 2425-2440, 2018.

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

[14] Z. Shao, Y. Duan, G. Coatrieux, J. Wu, J. Meng, and H. Shu, "Combining double random phase encoding for colour image watermarking in quaternion gyrator domain", *Optics Communications*, Vol. 343, pp. 56-65, 2015.

[15] M. R. Abuturab, "Multiple colour-image fusion and watermarking based on optical interference and wavelet transform", *Optics and Lasers in Engineering*, Vol. 89, pp. 47-58, 2017.

[16] S. Wang, X. Meng, Y. Yin, Y. Wang, X. Yang, X. Zhang, X. Peng, W. He, G. Dong, and H. Chen, "Optical image watermarking based on singular value decomposition ghost imaging and lifting wavelet transform", *Optics and Lasers in Engineering*, Vol. 114, pp. 76-82, 2019.

[17] Z. Shao, Y. Shang, Y. Zhang, X. Liu, and G. Guo, "Robust watermarking using orthogonal Fourier–Mellin moments and chaotic map for double images", *Signal Processing*, Vol. 120, pp. 522-531, 2016.

[18] M. D. Amiri, M. Meghdadi, and A. Amiri, "HVS-based scalable image watermarking", *Multimedia Tools and Applications*, Vol. 78, No. 6, pp. 7097-7124, 2019.

[19] M. Ghadi, L. Laouamer, L. Nana, and A. Pascu, "A blind spatial domain-based image watermarking using texture analysis and association rules mining", *Multimedia Tools and Applications*, Vol. 78, No. 12, pp. 15705-15750, 2019.

[20] A. Setyono, and D. R. I. M. Setiadi, "An Image Watermarking Method Using Discrete Tchebichef Transform and Singular Value Decomposition Based on Chaos Embedding", *International Journal of Intelligent Engineering and Systems*, Vol. 13, No. 2, pp. 140-150, 2020.

[21] A. Setyono and D. R. I. M. Setiadi, "Robust Video Watermarking using Tchebichef Transform and Singular Value Decomposition on the Selected Frame Based YCbCr Color Space", *International Journal of Intelligent Engineering and Systems*, Vol. 13, No. 6, pp. 432-441, 2020.

[22] T. Venugopal and V. S. K. Reddy, "Image watermarking using two level encryption method based on chaotic logistic mapping and Rivest Shamir Adleman algorithm", *International Journal of Intelligent Engineering and Systems*, Vol. 11, No. 6, pp. 271-281, 2018.