Nonlinear Dyn (2018) 93:1933–1951
https://doi.org/10.1007/s11071-018-4299-6

ORIGINAL PAPER

A new secure and robust watermarking technique based on logistic map and modification of DC coefficient

Shabir A. Parah · Nazir A. Loan · Asif A. Shah · Javaid A. Sheikh · G. M. Bhat

Received: 31 January 2017 / Accepted: 21 April 2018 / Published online: 4 May 2018

Abstract The proliferation of information and communication technology has made exchange of information easier than ever. Security and copyright protection of multimedia contents in such a scenario has become a major challenge for the research community round the globe. Digital watermarking has been found as an effective tool for protection and security of multimedia content. A secure and robust watermarking scheme based on DC coefficient modification in pixel domain and a modified logistic map is presented in this paper. The cover image is divided into 8×8 sub-blocks and instead of computing DC coefficient using discrete cosine transform (DCT), we compute DC coefficient of each block in spatial domain. Watermark bits are embedded by modifying DC coefficients of various blocks in spatial domain. The quantum of change to be brought in various pixels of a block for embedding watermark bit depends upon DC coefficient of respective blocks, nature of watermark bit (0 or 1) to be embedded and the adjustment factor. The security of embedded watermark has been taken care of by using chaotic encryption based on a generalized logistic map (GLM). We show that GLM has better properties like ergodicity, larger lyapunov exponent, uniform invariant density, mixing, higher range of bifurcation parameter etc., compared to basic logistic map. We exploit these properties of GLM for designing a secure robust, strong efficient cryptosystem to encrypt the watermark information before embedding it. Experimental investigations show that besides being highly secure the proposed technique is robust to both signal processing and geometric attacks. Further, the proposed scheme is computationally efficient as DC coefficient which holds the information is computed in pixel domain instead of using DCT on an image block.

Keywords Watermarking · Security · Chaotic encryption · Generalized logistic map · Robustness, computational complexity

S. A. Parah (✉) · N. A. Loan · A. A. Shah · J. A. Sheikh
Post Graduate Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, J&K 190006, India
e-mail: shabireltr@gmail.com

G. M. Bhat
Institute of Engineering and Technology, Zakura, J&K 190006, India

1 Introduction

As multimedia data transfer and usage has become widespread, the security and intellectual property rights (IPR) protection of digital multimedia contents from intervention by unauthorized users has become a critical issue [1]. The copying, reproduction and distribution of multimedia content has become easier than ever. Although various information scrambling schemes are being used to encrypt the multimedia content to avert adversary but the disguised look of the scrambled data enhances the chances of attack as it makes the attacker more suspicious. In the underlined circumstances some

serious work needs to be done not only to ensure security of multimedia content but also ensure its copyright protection. Digital watermarking is evolving as suitable technology to ensure security and protect multimedia data from copyright violations [2,3]. A digital watermark is a distinct data such as logo or signature etc., embedded in multimedia content like, audio, video or an image to prove its ownership or authenticate a given content.

Watermarking schemes are classified into many ways. Based on visibility of watermark the schemes are classified into visible and invisible watermarking categories. Usually invisible (imperceptible) watermarking techniques are employed for copyright protection. One of the important classifications of digital image watermarking techniques is based on the domain of embedding of the watermark. Depending on these criteria the watermarking schemes are divided into spatial and transform domain [5,6]. In spatial domain the watermark information is embedded directly in the pixels of the cover image. Spatial domain algorithms are computationally efficient and simple but susceptible to various geometric and image processing attacks [7,8]. Transform domain watermarking involves conversion of cover medium from pixel domain to frequency domain using a transformation tool. Some of the transforms utilized in transform domain watermarking are discrete cosine transform (DCT), fourier transform (FT) [8,9], discrete wavelet transform (DWT) [10,11], Contourlet transform and singular value decomposition (SVD) [12,13]. A successful watermarking scheme should exhibit the following characteristics to be counted as effective one:

(a) *Adjustability* The watermarking scheme should have the adaptability for varied degrees of robustness, perceptivity, and payload.
(b) *Robustness* The watermarking algorithm should be such that it should withstand all the attacks like noise addition, filtering, rotation, compression, cropping and others without compromising watermark.
(c) *Imperceptibility* The embedded watermark should not be perceived by human visual system.
(d) *Security* The watermarking algorithm should embed the watermark under control of a secure key, so that an adversary is unable to remove hidden data even having the knowledge of the embedding algorithm.
(e) *Computational complexity* The computational complexity of the watermarking algorithm should be least to facilitate real time processing.

This paper presents a secure, robust and computationally efficient watermarking algorithm based on the concept of logistic map and computing DC coefficient of DCT without actually using the DCT transform. The cover image is divided into 8×8 sub-blocks and instead of computing DC coefficient using discrete cosine transform (DCT), we compute DC coefficient of each block in spatial domain. Watermark bits are embedded by modifying DC coefficients of various blocks in spatial domain. The scheme as such mimics the behavior of a transform domain embedding approach in spatial domain; thus resulting in high robustness like in transform domain embedding approaches and less computational complexity of spatial domain embedding. The security of embedded watermark has been taken care of by using chaotic encryption based on a generalised logistic map (GLM). We show that GLM has better properties like ergodicity, larger lyapunov exponent (LE), uniform invariant density, mixing, higher range of bifurcation parameter etc. compared to basic logistic map.

2 Related prior work

Depending upon trade-off between various requirements like, robustness, imperceptibility, security, computational complexity and payload tremendous amount of work in the field of watermarking has been reported till date. Robustness is one of the most sought after parameters while developing a watermarking algorithm. A blind watermarking technique in DCT domain based on inter-block coefficient differencing has been reported by Parah et al. [14]. In this scheme the adjacent coefficient difference of two DCT coefficients has been put to use for watermark embedding. This scheme has been shown to be robust to both singular and hybrid attacks. In [15] blind and adaptive image watermarking scheme based on edge pixels has been reported. A two-level Contourlet transform and DCT in conjunction with a novel edge detection technique have been for watermark embedding. The robustness has been ensured by adding the watermark bits redundantly while as extraction is carried out using majority vote. A novel approach to watermarking based on space filling curve has been discussed in [16]. The

scheme makes uses of singular value decomposition (SVD) for multiple watermarks embedding to ensure copyright protection. The analysis carried out shows that the scheme is robust to various signal processing and geometric attacks. An adaptive digital image watermarking scheme based on frequency domain has been reported in [17]. The technique works on color images. To ensure security of watermark and better robustness Arnold transform and Hamming codes have been utilized. A fractional fourier transform (FrFT) based blind watermarking scheme has been reported in [18]. The experimental investigations show that the proposed algorithm has less robustness to JPEG compression. In [19] a robust and secure watermarking scheme has been reported. However, like [18] the performance of the technique to JPEG compression is poor. A DCT based watermarking algorithm using Arnold transform to reduce the correlation between pixels and improve security has been reported in [20]. A watermarking technique based on the concept of mathematical remainder is reported in [21]. The scheme however has lesser imperceptibility. In [22] a DCT based watermarking algorithm has been presented. The cover image is divided into 8×8 blocks followed by application of DCT to each block. The algorithm has been shown to be robust to various image processing and geometric attacks. The scheme however fails to utilize all the cover image blocks for watermark embedding and thus has a lower payload.

Security of watermark is one of the prime concerns while designing a watermarking algorithm. The nonlinear dynamics of chaos are currently being used to make watermarking systems secure and keep adversary at bay. May schemes involving secure watermark embedding based on chaos could be traced in [23–25]. In [23] a secure and blind watermarking scheme based on chaotic mixtures has been reported. The watermark has been encrypted using chaotic maps. The robustness has been taken care of by embedding in DWT approximation coefficients. A chaotic theory based watermarking system has been reported in [26]. The authors show that security strength of the system is increased may fold using Chaos. An intelligent watermarking algorithm based on chaotic map and quaternion wavelet transform (QWT) has been reported in [27]. A piecewise linear chaotic map has been used to scramble the watermark to increase its security. The authors demonstrate that the scheme has high robustness to commonly used signal processing attacks. A few relevant chaos based schemes for secure watermark embedding could be seen in [28,29]. Though chaos is being used as a potent tool for encrypting digital data. However use of chaos in digital domain leaves some clues for adversary to make cryptanalysis easy. Some of the recent works have reported how to use chaos for better security and avoid successful cryptanalytic attacks. Li et al. [41] have highlighted such issues to ensure that combination of encryption and chaos could be used in a more effective way. In [42] cryptanalysis of a famous chaotic scheme has been carried out. The work reports some key point's with regard to understanding of underlying encryption architecture for implementing a chaos based security system. In [43] it has been shown that correlation in multimedia data could also be used to enhance breaking performance. The cryptanalysis of work reported in [34] has been carried out in [44]. The authors conclude that multi-round encryption functions could also be prone to attacks. It is in place to mention that we don't make use of chaos alone for data security in the proposed system. The data to be transferred securely is firstly encrypted using chaos generated by proposed logistic map, followed by embedding it in cover medium. This way we provide two layers of security to the embedded data.

The current trend of implementation of watermarking algorithms involves embedding watermark in real time, wherein a watermark is embedded into cover image at the time of its capture. In such a scenario hardware implementation cost of the embedding algorithm plays an important role. A detailed analysis shows that FrFT, SVD, DWT and Rideglet transform are not a good for low cost and high speed hardware realization due to complexity involved in computing the transforms and data rate issues. Embedding watermark using DCT has proven to be better choice for real-time implementation due to the fact that joint picture expert group (JPEG) compression facility is inbuilt in image capturing elements wherein DCT is the primary step of this compression [30,31]. The above survey reveals that watermarking algorithms are developed either in pixel domain or transform. The chief benefit of former is reduced computational complexity and the later its robustness. In this paper a secure and robust technique for image watermarking is explored which has lesser computational complexity like spatial domain but offer robustness to various attacks as in transform domain. The security of the watermark has been ensured by encrypting it using a the GLM, which results in bet-

ter properties like ergodicity, larger lyapunov exponent (LE), uniform invariant density, mixing, higher range of bifurcation parameter etc. It has been successfully shown that a robust watermarking algorithm could be realized in spatial domain by embedding the watermark in DC component of DCT. It is pertinent to mention here that the DCT has not been put to use for computation of DC component of a given block, but, instead it has been computed in spatial domain. It is worth noting that a joint spatial and transform domain watermarking has already been reported in [32], but the authors make use of actual DCT transform to compute various coefficients including DC coefficient. The computation of the DC coefficients in spatial domain preserves the robustness of the scheme while simultaneously ensuring a low computational complexity.

3 Mathematical preludes

3.1 DC coefficients computation in pixel domain

Discrete cosine transform (DCT) transforms a set of real numbers in frequency domain. The DCT uses cosine function as its transformation kernel. DCT has been used extensively in numerous multimedia watermarking applications as compression standard JPEG is also built on it. For image transformation from pixel domain to spectral domain 2-D DCT transform is used. Inverse 2-D DCT is used for transforming in image from frequency to spatial domain. Consider an $R \times S$ image $f(x, y), (x = 0, 1, 2, \ldots, R-1, y = 0, 1, 2, \ldots, S-1)$, The forward 2-D DCT of $f(x,y)$ is given as

$$H(u,v) = \beta_u \beta_v \sum_{x=0}^{R-1} \sum_{y=0}^{S-1} f(x,y) \times \cos\frac{\pi(2x+1)u}{2R} \cos\frac{\pi(2y+1)v}{2S} \quad (1)$$

$$\beta_u = \begin{cases} \frac{1}{\sqrt{R}} & \text{for } u = 0 \\ \sqrt{\frac{2}{R}} & \text{for } 1 \le u < R-1 \end{cases} \quad (2)$$

$$\beta_v = \begin{cases} \frac{1}{\sqrt{S}} & \text{for } v = 0 \\ \sqrt{\frac{2}{S}} & \text{for } 1 \le v < S-1 \end{cases} \quad (3)$$

where R and S are the rows and columns of image $f(x, y)$, u and v are the horizontal and vertical frequency components $(u = 0, 1, 2, \ldots, R-1, v = 0, 1, 2, \ldots, S-1)$. The inverse DCT is given by

$$f(x,y) = \sum_{u=0}^{R-1} \sum_{v=0}^{S-1} \beta_u \beta_v H(u,v) \times \cos\frac{\pi(2x+1)u}{2R} \cos\frac{\pi(2y+1)v}{2S} \quad (4)$$

The DC coefficient in the DCT domain can be easily found using Eq. (1) and is given as

$$H(0,0) = \frac{1}{\sqrt{RS}} \sum_{x=0}^{R-1} \sum_{y=0}^{S-1} f(x,y) \quad (5)$$

It is evident from Eq. (5) that DC coefficient $H(0, 0)$ is simply averaged sum of all pixel values of $f(x, y)$ in the pixel domain. The basic procedure of adding a watermark in DCT domain involves addition of watermark information to various DCT coefficients, followed by usage of inverse DCT to obtain watermarked image. It is a proven fact that the energy of signal added to DC coefficient does not suffer any loss after the application of inverse DCT. In order to elaborate the results, please refer to [33]. The outline of the whole process is that embedding watermark into the DC coefficient in DCT domain can be easily replaced in the pixel domain.

3.2 DC component modification

We have already shown that the DC coefficient can be obtained by using arithmetic average of a given image block in spatial domain. Further, watermark embedding the DC component of DCT domain can be achieved by adjusting the value of pixel in the spatial domain appropriately. It is however pertinent to mention that the modified total of all the picture elements in pixel domain must equal the altered value of DC coefficient in transform domain. It is significant to find the updating value of every pixel in the pixel domain in accordance with changed value of DC component in the transform domain. From Eq. (4), the inverse DCT can be rewritten as

$$f(x,y) = \frac{1}{\sqrt{RS}} H(0,0) + f^{\sim}(x,y) \quad (6)$$

where $f^{\sim}(x, y)$ represents the reconstructed image from AC components. Assume that cover image is represented by number of non-overlapping blocks represented as

$$f(x, y) = f_{i,j}(m, n), 0 \le i < \frac{P}{b},$$
$$0 \le j < \frac{Q}{b}, 0 \le m, n < b, \quad (7)$$

where P and Q represent row and column dimensions of the cover image and $b \times b$ is size of each block (cover image is divided into $(i \times j)$ non-overlapped blocks). Let us assume that while embedding watermark bit into DC component of the (i, j)th block, the altered value of the said component is given by $\Delta\alpha_{i,j}$. Using Eqs. (4) and (5) the modified DC component of (i, j)th block is represented by

$$H'_{i,j}(0, 0) = H_{i,j}(0, 0) + \Delta\alpha_{i,j} \quad (8)$$

$$f'(m, n) = \frac{1}{b} H'_{i,j}(0, 0) + f^{\sim}_{i,j}(m, n) \quad (9)$$

where $H'_{i,j}(0, 0)$ represents the altered DC coefficient with alteration factor $\Delta\alpha_{(i,j)}$. It is further to be noted that $f^{\sim}_{(i,j)}(m, n)$ represents reconstructed image block from AC components while as $f\prime(m, n)$ represents cover image block with watermark data. From the above equations one can obtain

$$f'_{i,j}(m, n) = \frac{1}{b} H'_{i,j}(0, 0) + f'_{i,j}(m, n), \quad (10)$$
$$= \frac{1}{b}(H_{i,j}(0, 0) + \Delta\alpha_{i,j}) + f^{\sim}_{i,j}(m, n), \quad (11)$$
$$= \frac{\Delta\alpha_{i,j}}{b} + \frac{\Delta\alpha_{i,j}}{b}(C_{i,j}(0, 0) + g^{\sim}_{i,j}(m, n), \quad (12)$$
$$f'_{i,j}(m, n) = \frac{\Delta\alpha_{i,j}}{b} + f_{i,j}(m, n), \quad (13)$$

Above equations (10) to (13) specify that each pixel has to be modified using an alteration factor of $\frac{\Delta\alpha_{i,j}}{b}$.

4 Proposed system

The block diagram of proposed system is shown in Fig. 1. The information to be secured is firstly encrypted using chaotic encryption. A new GLM is used for chaos generation and providing first layer of security to the data to be secured. A detailed discussion about the proposed GLM and its properties is presented in sect. 4.1. The encrypted information has been embedded in the cover image imperceptibly by dividing each host image into 8×8 non-overlapping blocks. One bit of information has been embedded in each 8×8 block of cover image. Before embedding a watermark bit, the DC coefficient of each block has been computed without usage of DCT. The embedding and extraction algorithms are respectively presented in Sects. 4.2 and 4.3.

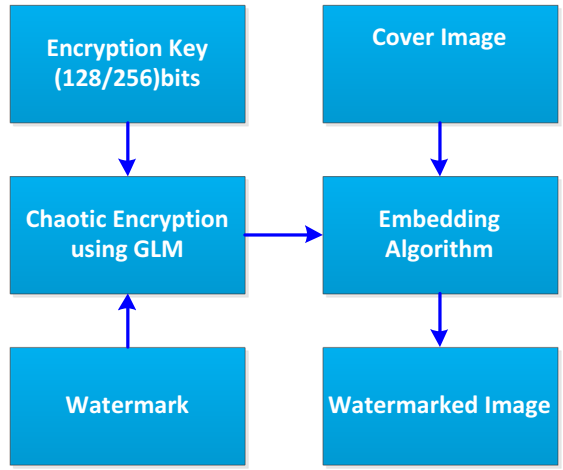

Fig. 1 Block diagram of the proposed scheme

The detailed description of the proposed scheme block diagram is as follows.

4.1 Chaotic encryption using proposed GLM

This section presents the proposed GLM, its properties and describes how it has been used for encrypting watermark information. The basic logistic map is presented as

$$y = \mu x(1 - x), \quad (14)$$

where $x \in [0,1]$ and '$a^0 \le 4$. Due to boundary crisis the map does not perform the chaotic behaviour after '$a^0 > 4$ and values diverge to attractor at infinity. We have generalized the Logistic map to what we refer to generalized logistic map (GLM). The GLM is defined as

$$y = \mu x(1 - x)MOD(1), \quad (15)$$

The Modular operation usage on basic logistic map as shown in Eq. 14, ensures that any value of μ (from zero to infinity) could be used for generation of chaos and thus there is no binding on the range of parameter 'μ'. This remarkable improvement would improve the security tremendously as it needs to scan the whole real

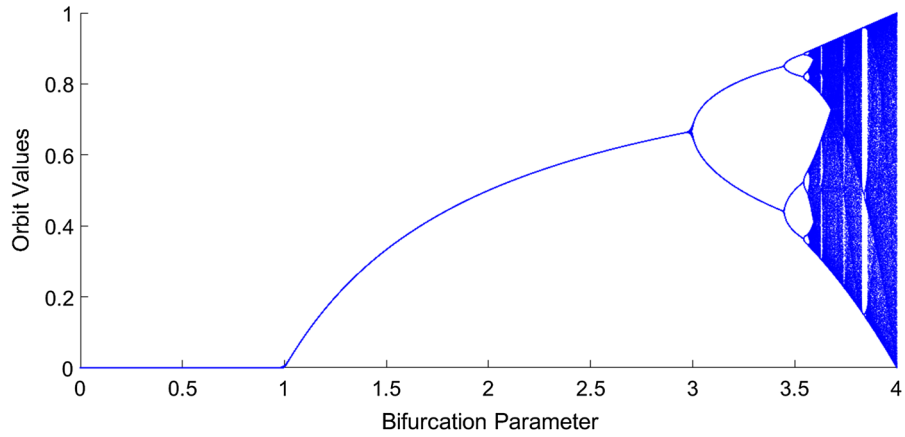

Fig. 2 Basic logistic map bifurcation diagram

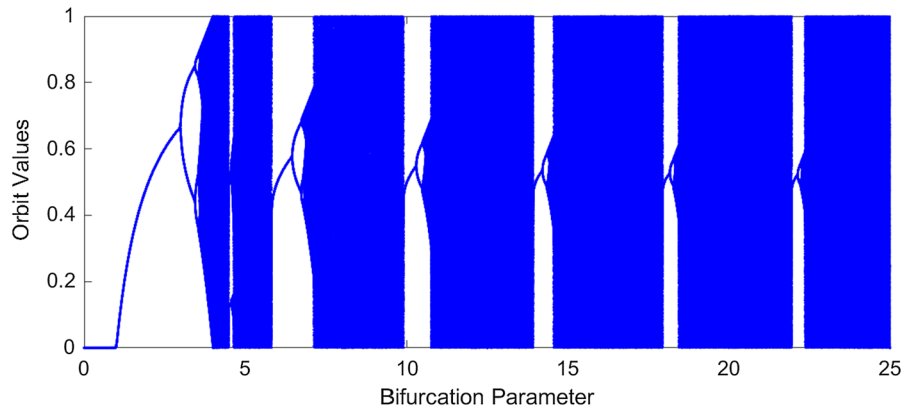

Fig. 3 Generalised logistic map bifurcation diagram (for 'μ' 0:50)

line for obtaining any significant information. MOD (1), modular arithmetic has been used to warrant the values lie in the interval (0, 1). We have tested the proposed GLM for encrypting the watermark for various tests and the results are presented below:

4.1.1 Bifurcation plots

The Bifurcation diagram of fundamental Logistic Map and GLM are respectively shown in Figs. 2 and 3. From Fig. 2 it is evident that the chaos breaks at $\mu > 4$ due to boundary crisis and values diverge to attractor at infinity.

The bifurcation plot of GLM [MOD (1)] as depicted in Fig. 3 results in chunks of like blocks towards right. As seen a periodic window appears at different values of parameter 'μ' and for different ranges and these ranges diminish as we increase value of parameter 'μ'. The most important feature of GLM, is that unlike fundamental logistic map any value 'μ' could be used for generation of chaos. This would tremendously help in development of a strong cryptosystem.

Figure 4 depicts the Bifurcation for negative and positive values of 'μ'. As could be seen the plot for negative values appears a tilted inversion to that of positive values of 'μ'.

4.1.2 Invariant density function (IDF)

The invariant density function (IDF) of fundamental logistic map described by Eq. (14) is like upward parabola with uneven distribution of frequency. The frequency is higher near 0 and 1. The IDF curve for rudimentary logistic map with interval 0.01 0.1 million iterations is shown in Fig. 5. The usage of modular operation [MOD (1)] on logistic map (GLM) results in change of non-uniform IDF curve to a near uniform curve as depicted in Fig. 6. It is to be noted that we have chosen '$\mu' = 110{,}000$ as an arbitrary higher value. This outstanding property could be used for development of proficient and resilient Cryptosystems.

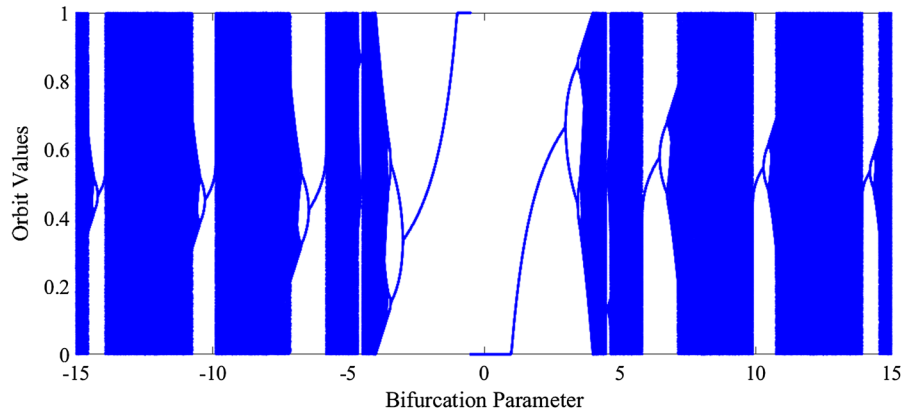

Fig. 4 Modular logistic map bifurcation diagram (for 'μ' - 20:20)

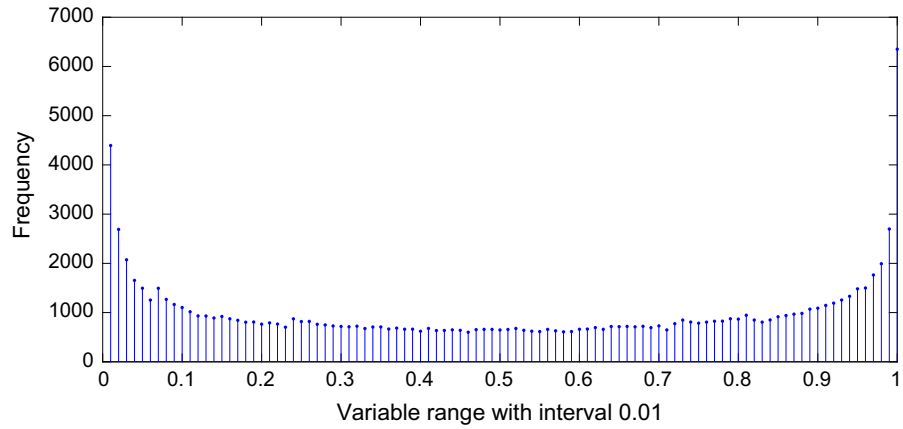

Fig. 5 IDF for a basic logistic map

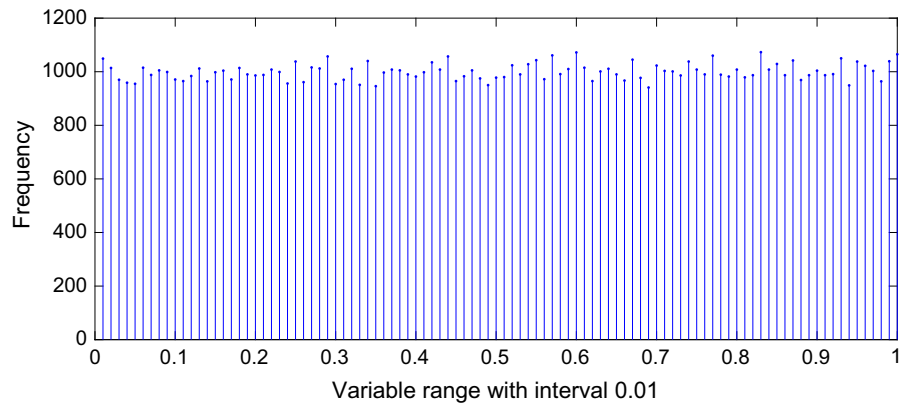

Fig. 6 IDF for generalized logistic map (For 'μ'= 110,000)

4.1.3 Lyapunov exponent (LE)

Chaos is characterized by fundamental quality that it has infinite sensitivity to initial conditions. Thus, any infinitesimal alteration in initial conditions results in different dynamics. The exponential divergence of Chaos is characterized by lyapunov exponent (LE). In the basic logistic map the maximum LE occurs near 4 as depicted in Fig. 7. But in GLM the LE keeps on increasing even after 'μ' > 4. The LE further increases to higher values in GLM as 'μ' is increased, as shown in Figs. 7 and 8. Figure 9 shows plot of LE for an arbitrarily chosen higher range ($110{,}451 \leq \mu \leq 110{,}458$) of system parameter'. This is an outstanding property of GLM and could result in an efficient strong Cryptosystems.

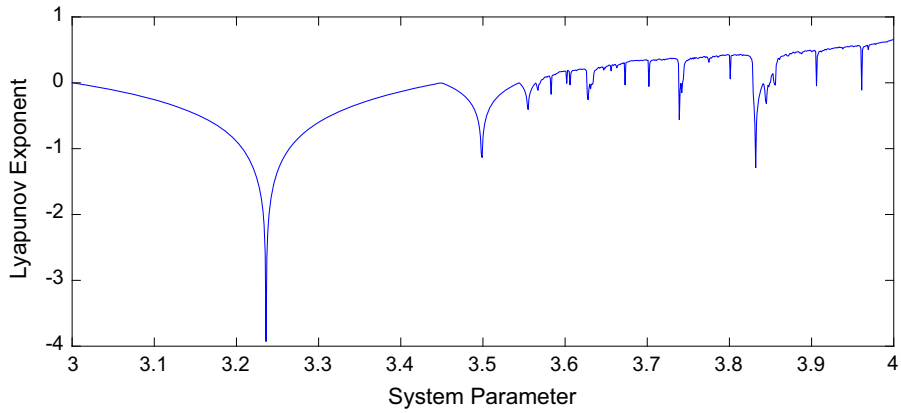

Fig. 7 Lyapunov exponent for basic logistic map in range $3 \leq \mu \leq 4$

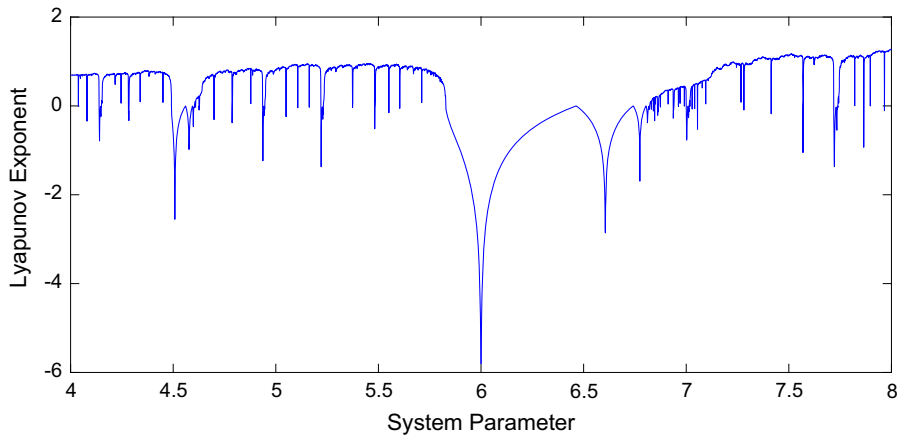

Fig. 8 Lyapunov exponent for GLM in the range $4 \leq \mu \leq 8$

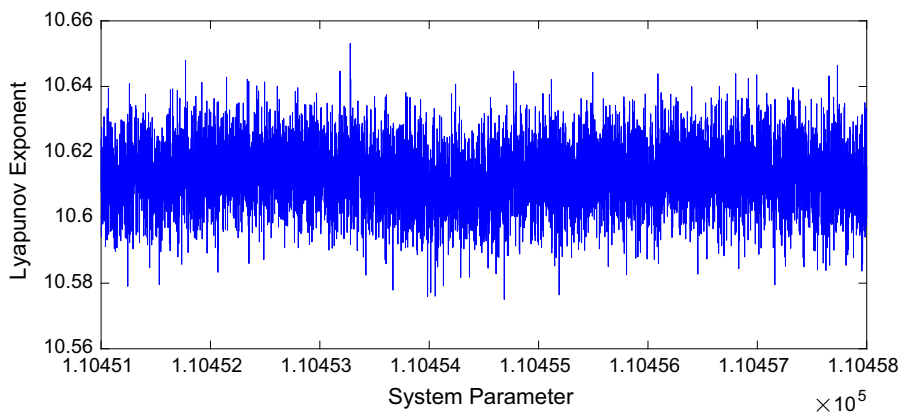

Fig. 9 Lyapunov exponent for GLM in the range $110{,}451 \leq \mu \leq 110{,}458$

4.2 Data encryption/decryption using proposed GLM

The watermark/ data to be secured is firstly encrypted using chaos generated by GLM prior to embedding in a cover image. The data set used for testing the encryption algorithm is ASCII printable characters as shown in Fig. 10.

4.2.1 Data encryption process

The encryption involves computation of chaotic map parameters like control parameter 'μ' and initial value x_0, and an intermediate value 'I' for confusion-diffusion operation. A secret key has been used to determine the parameters for two chaotic MLM based map

Code	Char	Code	Char	Code	Char	Code	Char	Code	Char	Code	Char
32	[space]	48	0	64	@	80	P	96	‘	112	p
33	!	49	1	65	A	81	Q	97	a	113	q
34	”	50	2	66	B	82	R	98	b	114	r
35	#	51	3	67	C	83	S	99	c	115	s
36	$	52	4	68	D	84	T	100	d	116	t
37	%	53	5	69	E	85	U	101	e	117	u
38	&	54	6	70	F	86	V	102	f	118	v
39	’	55	7	71	G	87	W	103	g	119	w
40	(	56	8	72	H	88	X	104	h	120	x
41	)	57	9	73	I	89	Y	105	i	121	y
42	*	58	:	74	J	90	Z	106	j	122	z
43	+	59	;	75	K	91	[	107	k	123	{
44	,	60	<	76	L	92	/	108	l	124	|
45	-	61	=	77	M	93	]	109	m	125	}
46	.	62	>	78	N	94	^	110	n	126	`
47	/	63	?	79	O	95	_	111	o	127	[backspace]

Fig. 10 Data set used for testing encryption algorithm

in a similar way as described in [34,35]. It is in place to mention that the schemes [34,35] have been analysed in [43,44] by E.Y. Xie et al. and Li. et al. The encryption of data is carried out in the following steps.

Step 1: Firstly, divide the 128-bit key into four blocks of 8 Hex digits each.

Step 2: Convert the HEX digits to their corresponding decimal values and divide by $2^{32}+1$. Let the 32-digit Hex key be K_1, K2, $K_3 \ldots K_{32}$. The four key blocks be KB_1, KB_2, KB_3, KB_4. The key blocks are defined as

$$KB_1 = (K_1, K_2 \ldots K_8)_{10}/(2^{32}+1), \quad (16)$$

$$KB_2 = (K_9, K_{10} \ldots K_{16})_{10}/(2^{32}+1), \quad (17)$$

$$KB_3 = (K_{17}, K_{18} \ldots K_{24})_{10}/(2^{32}+1), \quad (18)$$

$$KB_4 = (K_{25}, K_{26} \ldots K_{32})_{10}/(2^{32}+1), \quad (19)$$

Step 3: Generate two chaotic sequences (S1 & S2) from GLM using different parameters. Various control parameters and initial conditions for the two sequences are computed as

(a) *Calculation of parameters for S1* Control Parameter a_1

$$a_1 = B_1 + [KB_1 + KB_2 + I]MOD\ 1 * 0.001, \quad (20)$$

Initial Conditions x_{10}

$$x_{10} = [KB_2 + KB_3 + I]MOD\ 1, \quad (21)$$

(b) *Calculation of parameters for S2* Control Parameter a_2

$$a_2 = B_2 + [KB_1 + KB_2 + I]MOD\ 1 * 0.001, \quad (22)$$

Initial conditions x_{10}

$$x_{20} = [KB_3 + KB_4]MOD\ 1, \quad (23)$$

As GLM is chaotic over all range of control parameter the LE increases towards larger values of control parameter, we define B1 and B2 as the horizontal shift along the bifurcation diagram to any desired value as per the requirements of LE.

Step 4: Compute 'L' by first iterating the GLM using initial condition and control parameter of S2 as calculated in step 3. Here $X^{G2} = x_1^{G2}, x_2^{G2} \ldots x_L^{G2}$ with $x_1^{G2} \epsilon (0, 1)$, and decimal precision of 1015. $L = l + 1000$ where l is length of data to be encrypted (plaintext).

Step 5: Compute sum of product of chaotic values and plaintext as

$$\sum_{i=1}^{l} \left(P(i) * x_{L+1-i}^{G2} \right) MOD\ 1, \tag{24}$$

where $P(i)$ is plaintext characters for $i \in [1, l]$.

Step 6: Compute parameter H which has to be a printable character between (32–127). This is because the decimal values of the printable codes $\in$ (32–127) where

$$H = \begin{cases} MOD(round(S * 95), 128) \\ H + 32, \quad \text{if} \quad H < 32 \end{cases} \tag{25}$$

Finally, the value of 'I' used on map is

$$\boldsymbol{I} = \frac{\boldsymbol{H}}{\mathbf{127}}, \tag{26}$$

Since value of H is between [0,127], for it to be a printable ASCII character it has to lie in the range of (32–127). For H is less than 32, we add 32 to it to ensure its printability. 'H' is sent along with the ciphertext as $E_{\text{Last}} = H$, where E_{Last} is the last encrypted alphabet. At receiving end firstly 'I' is computed as $I = H/127$ finally 'I' together with key blocks KB_1 and KB_2 are used to compute parameters of S1. To decrypt ciphertext one must have knowledge of 'I' and Key.

Step 7: Generate another chaotic sequence S1 to add confusion step for the text to be encrypted. The chaotic sequence is given as $X^{G1} = x_1^{G1}, x_2^{G1} \ldots x_l^{G1}$ with $x_1^{G1} \epsilon (0, 1)$, and decimal precision of 10^{-15}. We choose T = 5000 and obtain confusion sequence as

$$Conf_i = round \left[(x_{(T-k+i)}^{G1}) * (k-1) \right] + 1, \tag{27}$$

where $i = 1, 2, 3 \ldots$ k and $Conf \in [1, k]$.

Step 8: Introduce diffusion mechanism

$$D_i = round \left[(x_{1(5000-L_n+i)}^{G1}) * 94 \right] + 1, \tag{28}$$

We iterate the GLM for sequence S1 with $T = 5000$ times and skip first $5000 - L_n$ iterations, where L_n is length of plaintext. Afterwards from $T = 5000 - L_{n+1}$, we use each chaotic value x_l^{G1}. Here $i = 1, 2, 3 \ldots k$ and $D_i \in$ [1,95].

Step 9: The encrypted data is finally given as

$$E_i = round \{ \left[P(Conf_i) - 32 + D_i \right] \mathbf{MOD}\ 95 \} + 32, \tag{29}$$

where $E_i \in$ (32,127) is encrypted/cipher text. The flow chart of the encryption algorithm is shown in Fig. 11a.

4.2.2 Decryption process

This process involves complete reverse operation as in case of encryption. Firstly 'I' is extracted from E_{Last} by involving by using $E_{\text{Last}} = 127 * I$. Iterate GLM using initial condition and system parameter value of sequence S1 and S2 in the same way as at transmitter side using pre-shared key blocks. Finally, the decrypted data is given by

$$\text{PT}_i = \{ [P(\text{Conf}_i) - 32 + D_i] \mathbf{MOD}\ 95 \} + 32, \tag{30}$$

where $i = 1, 2, 3 \ldots k$, $PT_i \in [32, 127]$ is plaintext. The flow chart of the decryption process is shown in Fig. 11b. Besides encrypting the text using the above algorithm we have also used it for image encryption as well. It is to be noted that for encrypting an $m \times n$ sized binary image we firstly convert it into a row vector of size $1 \times mn$, the encrypted data pertaining to the row vector is again reshaped to obtain encrypted image of size $m \times n$. Figure 12 shows a 64×64 binary watermark encrypted using the GLM scheme. Figure 12a, b show the original watermark and its encrypted version using chaotic encryption based on GLM.

4.3 Watermark embedding

The watermark embedding is carried out as follows:

(i) Read the cover image.

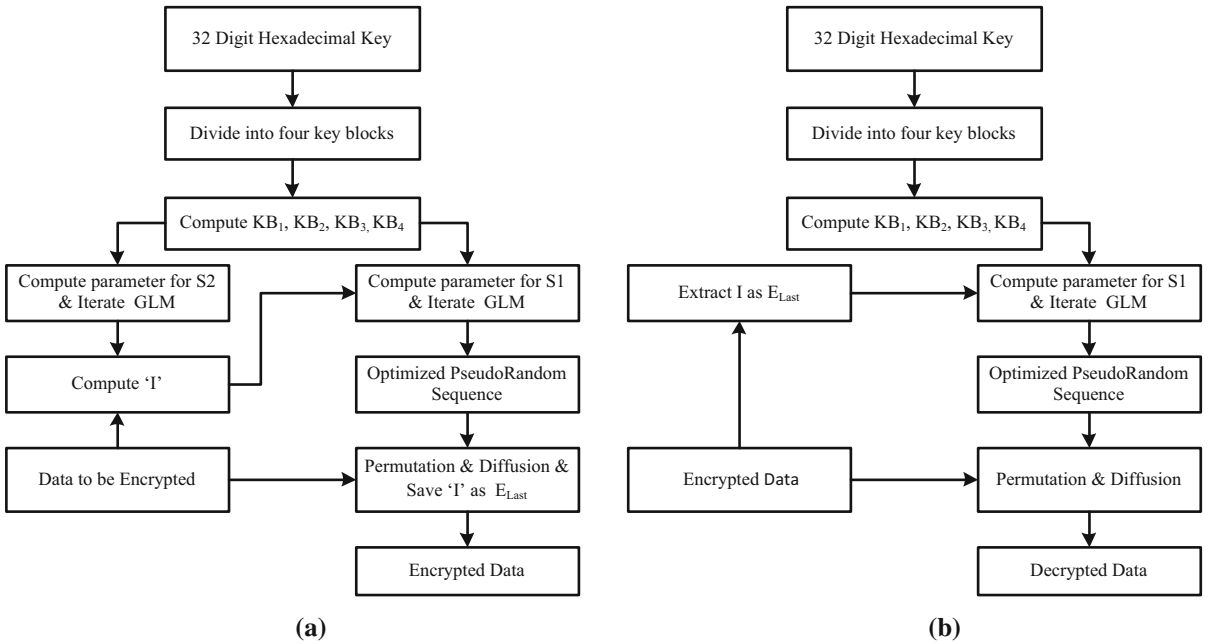

Fig. 11 Flow charts **a** encryption algorithm, **b** decryption algorithm

Fig. 12 **a** Original watermark. **b** Encrypted watermark

(ii) Divide the cover image into 8×8 non-overlapping blocks. (iii) Use GLM to encrypt the watermark.

(iii) Use GLM to encrypt the watermark.

(iv) Calculate DC coefficient $H_{i,j}(0,0)$ of each block.

(v) Compute alteration factors magnitudes ΔF1 and ΔF2 as

$$\Delta F1 = \begin{cases} 0.5\psi, & \text{if } ew(i,j) = 1 \\ -0.5\psi, & \text{if } ew(i,j) = 0 \end{cases}, \tag{31}$$

$$\Delta F1 = \begin{cases} -1.5\psi, & \text{if } ew(i,j) = 1 \\ 1.5\psi, & \text{if } ew(i,j) = 0 \end{cases}, \tag{32}$$

(vi) Use alteration factors ΔF1 and ΔF2 to compute the quantized coefficient values as

$$H_1 = 2k\psi + \Delta F1 \text{ and } H_2 = 2k\psi + \Delta F2$$

where $k = floor(ceil(H_{i,j}(0,0)/2\psi$
Then, compute $H'_{i,j}(0,0)$ for embedding the watermark in $H_{i,j}(0,0)$ using the following expression:

$$H'_{i,j}(0,0) = \begin{cases} H_2 & \text{if } \text{abs}(H_{i,j}(0,0) - H_2) \\ & \quad < \text{abs}(H_{i,j}(0,0) - H_1) \\ H_1 & \text{else} \end{cases} \tag{33}$$

where

$$\Delta H_{i,j}(0,0) = H'_{i,j}(0,0) - H_{i,j}(0,0), \tag{34}$$

(vii) To obtain the watermarked image, add $\Delta H_{i,j}(0,0)/8$ to every pixel of the block.

4.4 Watermark extraction

The watermark extraction algorithm is as follows:

(i) Watermarked image is divided into non-overlapped 8×8 blocks.

(ii) Compute DC coefficient $H_{i,j}(0,0)$ of each block directly as done during embedding.

(iii) Compute the encrypted watermark by utilizing ψ as

$$e(i,j) = \text{mod}\left(\text{ceil}\left(\frac{H_{i,j}(0,0)}{\psi}\right), 2\right), \tag{35}$$

(iv) For successful decryption of watermark use same key as one used during encryption.

5 Experimental results and discussions

The proposed system has been analysed in terms of various subjective and objective image quality metrics for watermarked image quality evaluation besides carrying out security analysis like key space test, key sensitivity test, differential attacks test etc. The main requirements of a digital image watermarking systems are imperceptibility, robustness, computational complexity and security. It is in place to mention here that we have evaluated our scheme on on i3-2350 processor with 2 GB using MATLAB 7 .0 software running on windows platform.Following subsections present the analysis of our system with respect to these important parameters:

5.1 Imperceptibility analysis

Imperceptibility refers to ability of a watermarking system to produce a watermarked image that seems to be same as cover image under subjective analysis. We present subjective and objective experimental results as obtained in our scheme. It is pertinent to mention here that we have cover images of 512×512, while as size of watermark used for embedding is 64×64. Various host images and corresponding watermarked images obtained using our technique, are presented in Fig. 13. Table 1 shows the image quality metrics like peak signal to noise ratio (PSNR) and normalized cross-correlation (NCC). The image quality metrics have been defined as in [36–38,40].

The subjective quality results are testimony to the fact that our scheme is capable of producing high quality watermarked images. The average PSNR values of above 42 dB and NCC value of unity indicate that our scheme yields high quality watermarked images. Figure 14 presents a comparison of the PSNR of our technique with some of the state-of-art schemes for test image 'Lena'.

It is clear that the proposed scheme outperforms all the techniques under comparison. Table 2 shows comparison of our scheme with Parah et al. for various test images. The results show the superiority of the proposed scheme.

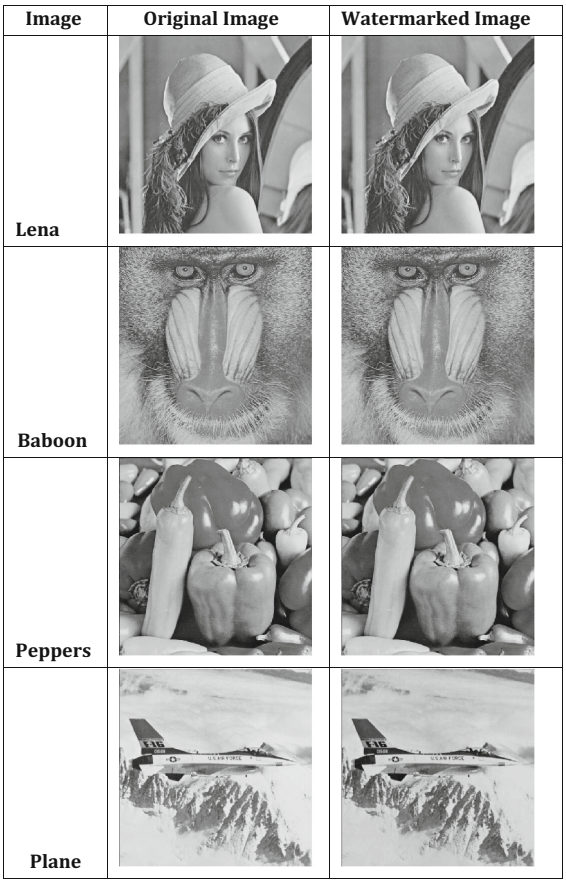

Fig. 13 Original images and their corresponding watermarked versions

Table 1 Various image quality metrics for watermarked images

Image	PSNR(dB)	NCC
Lena	42.85	1.0000
Baboon	42.91	1.0000
Peppers	42.85	1.0000
Plane	42.70	1.0000
Average	42.83	1.0000

5.2 Robustness analysis

We have subjected the watermarked images to various image processing and geometric attacks in order to investigate the robustness of our technique. The subjective quality of watermarked images, when subjected to various attacks, for test image Lena are shown in Fig. 15. Table 3 shows average of various

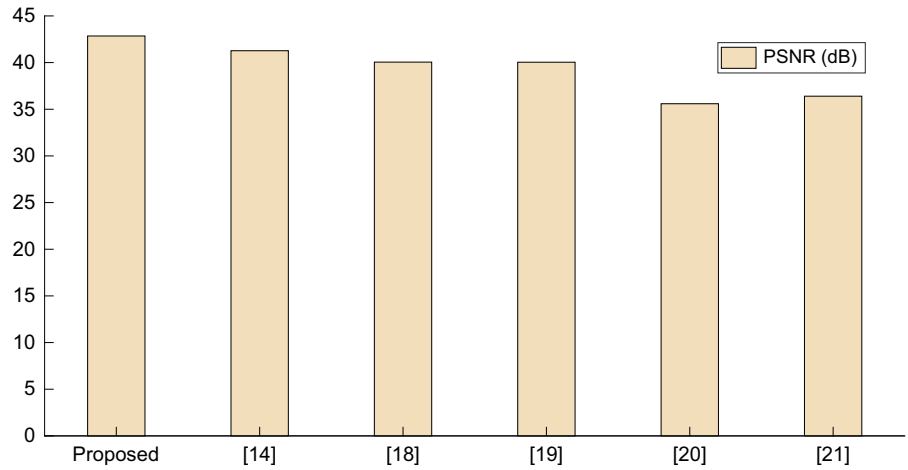

Fig. 14 Comparison of proposed scheme with state-of art- for "Lena"

Table 2 Comparison of proposed scheme with Parah et al. [14, 40]

Image	PSNR(dB)		
	Parah et al. [14]	Patra et al. [40]	Proposed
Lena	41.27	41.41	42.85
Baboon	41.21	41.93	42.91
Peppers	41.84	NA	42.85
Plane	41.17	41.40	42.70
Average	41.37	41.58	42.83

objective quality parameters obtained for watermarked images. It is pertinent to mention that average values indicate the averages for Lena, Baboon, Peppers and Plane.

It is worth to mention here that NCC and BER have been computed between original and extracted watermarks and PSNR between host and Watermarked images.

5.3 Discussions on robustness

The following section briefly discusses the robustness of our scheme to various attacks in light of the results depicted in Table 3.

(i) *Gaussian noise* We have tested our scheme for additive white Gaussian noise with variance of 0.0002. The results show that average BER for this attack is just above 14 %, showing that our technique is robust to this attack.

(ii) *Salt and pepper attack* Salt and Pepper attack of density 0.01 was carried out and the average BER values obtained are above 27%. The results show that the scheme is relatively fragile to this attack.

(iii) *Histogram equalization* The results show that our scheme is not robust to this attack as the BER values are in the range of 43%.

(iv) *Median filtering* Median Filtering attack with a kernel of (3×3) carried out on the watermarked images show that our scheme is highly robust to this attack. It is substantiated by low average BER of about 5%.

(v) *Low pass filtering* Low Pass Filtering attack with filter kernel size of (3×3) was carried out on watermarked images. The scheme shows an average error of about 8% and such is robust to this attack.

(vi) *Sharpening* We have subjected the scheme sharpening attack of kernel (3×3). The average BER values observed are above 30% indicating that the scheme is less robust to this attack.

(vii) *Rotation* We have subjected the watermarked images obtained in the proposed technique to rotation of various degrees. It was observed that our technique robust to this attack as depicted by the low average BER values of 4–19% for a rotation from 1° to 45°.

(viii) *JPEG Compression* We have extensively tested the proposed technique for JPEG compression under various quality factors. We have varied the Quality factor from 10 to 80. The experimental investigations reveal that our technique is highly robust. As is evident from Table 3 BER varies

Fig. 15 Subjective quality of 'Lena' for various attacks. **a** Median filtering (3×3). **b** Salt and pepper ($d = 0.01$). **c** Histogram equalization. **d** Rotation (10°). **e** Cropping center. **f** Gaussian noise ($\nu = 0.0002$). **g** JPEG Compression ($QF = 80$). **h** Low pass filtering (3×3). **i** Sharpening (3×3)

from 6 to 45% for quality factor values in the range of 40–10. The BER significantly reduces and its value is zero for a quality factor of 50 or above. We conclude that our technique is completely robust to JPEG compression for a quality factor of 50 or above.

ix) *Cropping* We have cropped the watermarked images at various corners and centre. The results shown in Table 3 that our scheme successfully with stands all sorts of cropping We have compared various robustness parameters of our technique with Parah et al., [14] and Das et al. [22]. The comparison results are shown in Tables 4 and 5. The results depicted in Tables 4 and 5 show superiority of our scheme.

5.4 Computational complexity

This section presents computational complexity analysis of our scheme in terms of time required for watermark embedding and extraction. For evaluation and testing purpose, we have embedded a 64×64 watermark in various 512×512 test images. A comparison of the proposed scheme for embedding time, extraction time and total time with that using conventional DCT based DC coefficient modification has been shown in Table 6. It is evident from the results that our scheme out performs the conventional DCT based embedding scheme in terms of both embedding and extraction time. The total time for embedding and extraction of our scheme is about eight times smaller compared to the conventional DCT based embedding scheme. The

Table 3 Average image quality parameters after different attacks

Attack	PSNR(dB)	BER	NCC
No attack	42.8375	0	1.0000
Guassian noise ($v = 0.0002$)	29.9921	0.1416	0.9768
Salt and pepper noise ($d = 0.01$)	25.7822	0.2719	0.9476
Histogram equilisation	18.4125	0.4393	0.8609
Median filtering (3×3)	34.0120	0.0535	0.9809
Low pass filtering	29.7890	0.0852	0.9042
Sharpening (3×3)	24.5413	0.3230	0.9291
JPEG (quality factor)			
10	28.8971	0.4580	0.8127
20	29.3351	0.2912	0.9361
30	30.1578	0.0635	0.9945
40	31.3456	0.0059	0.9999
50	32.7814	0	1.0000
60	33.1820	0	1.0000
70	34.0012	0	1.0000
80	35.1522	0	1.0000
Rotation (°)			
1	42.53171	0.0412	0.9899
10	42.5720	0.0718	0.9821
45	42.0031	0.1949	0.9879
Cropping			
Center	42.4134	0.0991	0.9957
Top left corner	42.6332	0.2109	1.0000
Bottom left corner	42.9111	0.2231	0.9999
Top right corner	42.2347	0.2015	1.9999
Bottom right corner	42.2153	0.0321	0.9982

Table 4 Robustness comparison in terms of NCC of proposed scheme with Das et al [22], Parah et al., [14] for 'Lena'

Attack type	Normalised Cross-corelation (NC)		
	Parah et al. [14]	Das et al. [22]	Proposed
Median filtering (3×3)	0.9445	0.9118	0.9809
Salt and pepper noise (0.01)	0.8598	0.8122	0.9476
Histogram equlization	0.9665	0.9353	0.8609
AWGN(0.0001)	0.9375	0.8816	0.9728

reason of better performance of our scheme is that we compute DC coefficient of each block in spatial domain according to Eq. 5 (without using DCT) while as use of DCT and IDCT in the conventional transform domain embedding scheme increases the computational complexity.

Table 5 Robustness comparison of proposed scheme with [14, 22] for cropping attack for test Image 'Lena'

Cropped area	Normalised cross-corelation (NC)		
	Das et al. [22]	Parah et al. [14]	Proposed
25% Top-left corner	0.9954	0.9986	1.0000
25% Top-right corner	0.9973	0.9980	0.9999
25% Bottom-left corner	0.9924	0.9989	0.9999
25% Bottom-right corner	0.9981	0.9980	0.9982

5.5 Security analysis

5.5.1 Key space analysis

The proposed technique uses a 128 bit key resulting into a possibility of 2^{128} different Keys. If we assume that computational power available with adversary is such that he is capable of generating one key/μ s. With such a power it will take him 5.4×10^{18} years to break our algorithm. Thus our technique is highly secure to Brute Force Attack. Further our system can be easily upgraded to use a key size of 256 bits thus making it impossible to break it using Brute force attack.

5.5.2 Key sensitivity analysis

We have subjected our scheme to Key sensitivity test which analysis its ability to generate two different cipher text/encrypted watermarks when two pieces of plain text/original watermark are encrypted using same key. Further, in case of one bit error in key we should not be able to decrypt the text or watermark data successfully. We used the key (K = 123456785CABCDEF5534567890ABCEFB) for encryption of the plain text as shown in Fig. 16a–c show the encrypted data with same key K and one bit erroneous version of K. The decrypted data with one bit error in Key is shown in Fig. 16d. As seen the cryptograms obtained with actual key and its one bit

Table 6 Robustness comparison of proposed scheme with [14,22] for cropping attack for test Image 'Lena'

Images	Proposed scheme			Conventional DCT Embedding		
	Embedding time (s)	Extraction time (s)	Total time (s)	Embedding time (s)	Extraction time (s)	Total time (s)
Lena	0.4844	0.0469	0.5313	1.5781	2.5	4.0781
Baboon	0.6563	0.0469	0.7031	1.5	2.4219	3.9219
Plane	0.4063	0.0469	0.4531	1.5469	2.7031	4.25
Peppers	0.51	0.0.0625	0.5625	1.5469	2.5156	4.0625
Average	0.51425	0.0508	0.5625	1.5429	2.5351	4.0781

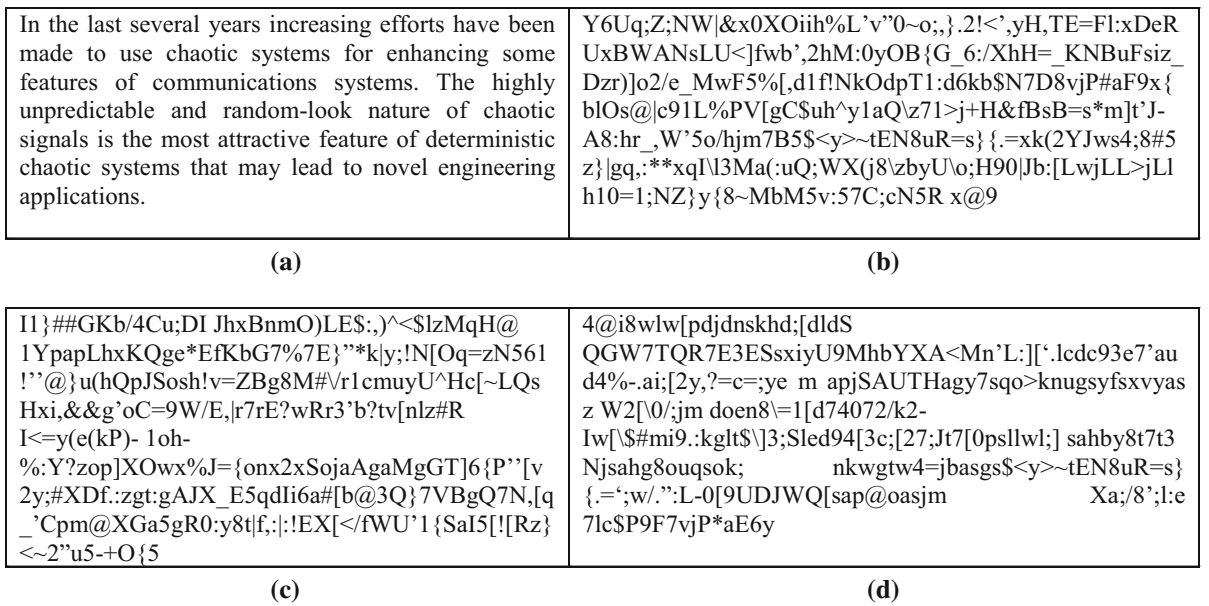

Fig. 16 Plaintext, encrypted text and decrypted text with one bit change in the key. **a** Plaintext. **b** Ciphertext with key (K = 123456789$CABCDEF$5534567890$ABCEFB$). **c** Ciphertext with one bit change in key (K = 123456789$CABCDEF$5534567891$ABCEFB$). **d** Decrypted text with one bit change in key (K = 123456789$CABCDEF$5524567890$ABCEFB$)

erroneous version are completely different, showing that our scheme has very high key sensitivity. Similarly we are unable to get any clue of information from the deciphered text when key is having one bit error.

5.5.3 Frequency analysis

We have carried out the histogram analysis of our scheme encrypting a chunk of information of about 1000 characters. The histogram of plaintext and encrypted text is shown in Figs. 17 and 18 respectively. The uniformity of the histogram shows that our scheme is capable of averting any statistical attacks.

5.5.4 Information entropy analysis

The diffusion round for an encryption system should be highly efficient to ensure that all values of plaintext symbols be changed modified in order to avert Entropy attack. The entropy of information is computed as

$$H(m) = -\sum_{i=0}^{2^N-1} p(m_i)\log_2\frac{1}{p(m_i)}, \tag{36}$$

where N represents number of information bits, $p(m_i)$ represents probability of message bits (m_i). In an ideal situation the entropy for 2^N symbols should be N. We

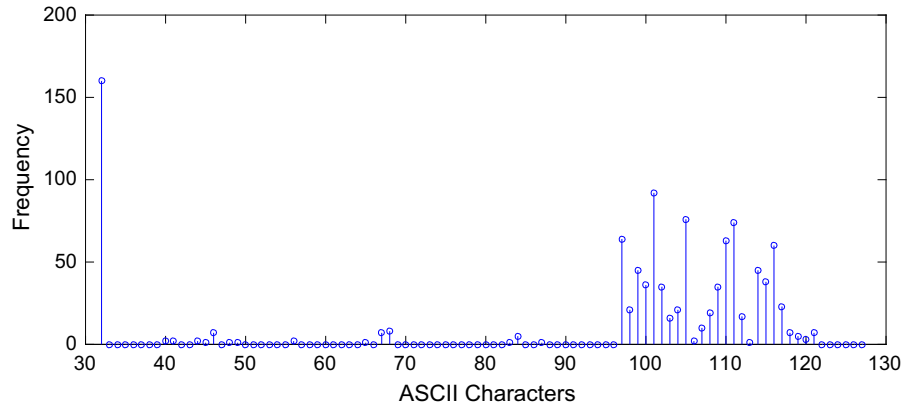

Fig. 17 Histogram for plaintext

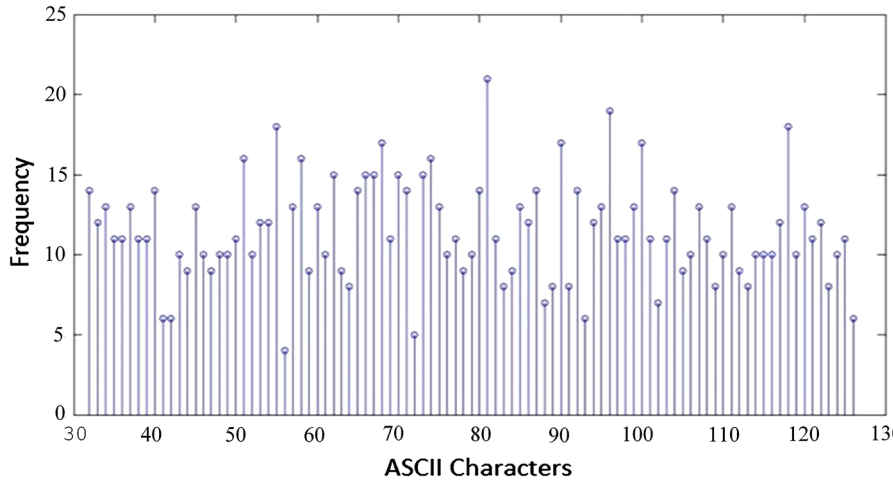

Fig. 18 Histogram for ciphertext

have tested our scheme for 95 symbols, so maximum entropy is $H = 6.56$. The plaintext entropy as calculated is $H(\text{Plaintext}) = 4.3019$ whereas the encrypted text entropy using our technique is $H(\text{Ciphertext}) = 6.4928$ which is close to ideal entropy. Thus our scheme is immune to this attack as well.

5.5.5 Differential analysis

Differential analysis is used for checking the algorithm sensitivity to alteration in plain text. Usually in this attack one character of plaintext is altered (by decrementing or incrementing it by one bit) and then encrypted. The two results are compared. A secure encryption scheme causes significant changes in the ciphertext with one minor change in the plaintext and hence could resist chosen plain text attack or known plaintext attack. The objective analysis for this attack is carried out using Two scales for objective analysis of this attack are Net Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) as defined in [34]. The experimental investigations reveal the following values for NCPR and UACI

$$\textbf{NPCR} = 99.0103\%; \textbf{UACI} = 34.821\%$$

5.5.6 Comparison of results

The proposed scheme based on GLM is compared with one based on fundamental logistic map for various system parameters keeping the test text same as reported in [39]. The results have been shown in Table 7. The results clearly show that our scheme performs better.

5.6 Conclusion

A secure and robust watermarking scheme based on DC coefficient modification in spatial domain and a modified logistic map (GLM) has been presented in this

Table 7 Comparison of GLM with [39]

Parameters	Scheme reported in [39]	Proposed GLM scheme
Key	128 bits	128 bits
Entropy	6.481	6.5242
UACI (%)	33.31	34.821
NPCR (%)	98.85	99.0103
Encryption time (s)	0.125709	0.116468
Decryption time (s)	0.107431	0.102004

paper. Cover image was divided into 8×8 sub-blocks and DC coefficient of each block computed in in spatial domain instead of using Discrete Cosine Transform (DCT). Watermark bits were embedded by modifying DC coefficients of various blocks in spatial domain. The quantum of change brought in various pixels of a block for embedding watermark bit depends upon DC coefficient of respective blocks, nature of watermark bit (0 or 1) to be embedded and the adjustment factor. The security of embedded watermark was taken care of by using chaotic encryption based on the Generalised Logistic Map (GLM). We showed that GLM has better properties like ergodicity, larger Lyapunov Exponent (LE), uniform invariant density, mixing, higher range of bifurcation parameter etc. compared to basic logistic map. The properties of GLM were exploited for designing a secure robust, strong efficient cryptosystem to encrypt the watermark information before embedding it. Experimental investigations revealed that besides being highly secure the proposed technique is robust to most of the signal processing and geometric attacks. Further, the proposed scheme is computationally efficient as DC coefficient which holds the information has been computed in pixel domain instead of using DCT on an image block. Though the scheme has been found secure and highly robust to many attacks like, JPEG compression, Low Pass Filtering, Median Filtering, cropping, and rotation but robustness to attacks like histogram equalization and sharpening is poor. As a part of future work, we aim to improve the algorithm so as to improve its performance to these attacks as well.

Acknowledgements The authors acknowledge the support rendered by University Grants Commission (UGC) Government of India under its SAP programme for conduct of this work.

References

1. Li, C., Lin, D., Lu, J., Hao, F.: Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. (2017). arXiv:1711.01858
2. Djurovic, I., Stankovic, S., Pitas, I.: Digital watermarking in the fractional Fourier transformation domain. J. Netw. Comput. Appl. **24**, 167–173 (2001)
3. Parah, S.A., Sheikh, J.A., Hafiz, A.M., Bhat, G.M.: A secure and robust information hiding technique for covert communication. Int. J. Electron. **102**, 1253–1266 (2014)
4. Shabir, A.P., Javaid, A.S., Bhat, G.M.: Data hiding in scrambled images: a new double layer security data hiding technique. Comput. Electr. Eng. **40**, 70–82 (2014)
5. Parah, S.A., Javaid, A.S, Farhana, A., Bhat, G.M.: On the realization of robust watermarking system for medical images. In: 12th IEEE India International Conference (INDICON) on Electronics, Energy, Environment, Communication, Computers, Control (E3-C3), pp. 1–6. Jamia Millia Islamia, New Delhi (2015)
6. Shabir, A.P., Javaid, A.S., Bhat, G.M.: On the realization of a secure, high capacity data embedding technique using joint top-down and down- top embedding approach. Elixir Comp. Sci. Eng. **49**, 10141–10146 (2012)
7. Shabir, A.P., Javaid, A.S., Bhat, G.M.: High capacity data embedding using joint intermediate significant bit and least significant technique. Int. J. Inf. Eng. Appl. **2**, 1–11 (2013)
8. Cintra, J., Dimitrov, S., Oliveira, M., Campello, M.: Fragile watermarking using finite field trigonometrical transforms. Signal Process. Image Commun. **24**(7), 587–597 (2009)
9. Liu, Y., Zhao, J.: A new video watermarking algorithm based on 1D DFT and Radon transform. Signal Process. **90**(2), 626–639 (2010)
10. Ghouti, L., Bouridane, A., Ibrahim, M., Boussakta, S.: Digital image watermarking using balanced multi-wavelets. IEEE Trans. Signal Process. **54**(4), 1519–1536 (2106)
11. Lu, W., Sun, W., Lu, H.: Novel robust image watermarking based on subsampling and DWT. Multimed. Tools Appl. **60**(1), 31–46 (2012)
12. Lai, C., Tsai, C.: Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans. Instrum. Meas. **59**(11), 3060–3063 (2010)
13. Chen, R., Luo, Y., Lan, Y., Alsharif, M.: A new robust digital image watermarking algorithm based on singular value decomposition and independent component analysis. J. Con. Inf. Tech. **8**(5), 530–537 (2013)
14. Parah, S.A., Sheikh, J.A., Bhat, G.M.: Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. Digit. Signal Process. **53**, 11–24 (2016)
15. Fazlali, H.R., Samavi, S., Karimi, N., Shirani, S.: Adaptive blind image watermarking using edge pixel concentration. Multimed. Tools Appl. **76**, 3105 (2016). https://doi.org/10.1007/s11042-015-3200-6
16. Bhatnagar, G., Wu, Q.M.: A new robust and efficient multiple watermarking scheme. Multimed. Tools Appl. **74**, 8421–8444 (2015)
17. Kalra, G.S., Talwar, R., Sadawarti, H.: Adaptive digital image watermarking for color images in frequency domain. Multimed. Tools Appl. **74**, 6849–6869 (2015)

18. Lang, J., Zhang, Z.: Blind digital watermarking method in the fractional Fourier transform domain. Opt. Lasers Eng. **53**, 112–121 (2014)
19. Guo, J., Zheng, P., Huang, J.: Secure watermarking scheme against watermark attacks in the encrypted domain. J. Vis. Commun. Image Represent. **30**, 125–135 (2015)
20. Ma, F., Zhang, J., Zhang, W.: A blind watermarking technology based on DCT do-main, In: Proceedings of the IEEE International Conference on Computer Science and Service System, CSSS, 2012, pp. 398–401 (2012)
21. Lin, S., Shie, S., Guo, J.Y.: Improving the robustness of DCT-based image watermarking gainst JPEG compression. Comput. Stand. Interfaces **32**, 54–60 (2010)
22. Das, C., Panigrahi, S., Sharma, V.K., Mahapatra, K.K.: A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. Int. J. Electron. Commun. **68**, 244–253 (2014)
23. Niansheng, L., Huajian, L., Huaiyu, D., Donghui, G., Deming, C.: Robust blind image watermarking based on chaotic mixtures. Nonlinear Dyn. **80**, 1329–1355 (2015)
24. Sajjad, S., Jamal, T.S., Iqtadar, H.: An efcient scheme for digital watermarking using chaotic map. Nonlinear Dyn. **73**, 1469–1474 (2013)
25. Seyyed, M.R., Farschi, H.: A novel chaotic approach for information hiding in image. Nonlinear Dyn. **69**, 1525–1539 (2012)
26. Amir, A., Adil, M.S., Jameel, A., Iqtadar, H.: A technique for digital steganography using chaotic maps. Nonlinear Dyn. **75**, 807–816 (2014)
27. Laiying, L., Dong, N., Siping, C., Tianfu, W., Feng, Z.: Optimal image watermarking scheme based on chaotic map and quaternion wavelet transform. Nonlinear Dyn. **78**, 2897–2907 (2014)
28. Chen, P., Yu, S., Zhang, He, J., Lin, Z., Le, C., Lu, J.: ARM-embedded implementation of a video chaotic secure communication via WAN remote transmission with desirable security and frame rate. Nonlinear Dyn. **86**, 725–740 (2016)
29. Zhao, J., Wang, S., Chang, Y., Li, X.: A novel image encryption scheme based on an improper fractionalorder chaotic system. Nonlinear Dyn. **80**, 1721–1729 (2015)
30. Elbadri, M., Peterkin, R., Groza, V., Ionescu, D., Saddik, A.E.: Hardware support of JPEG. In: Proceedings of Canadian Conference on Electrical and Computer Engineering pp. 812–815 (2005)
31. Wallace, G.K.: The JPEG still picture compression standard. IEEE Trans. Consum. Electron. **38**, 18–24 (1992)
32. Shih, F.Y., Wu, S.Y.: Combinational image watermarking in the spatial and frequency domains. Pattern Recogn. **36**(4), 969–975 (2003)
33. Su, Q., Ni, Y., Wang, Q., Sheng, G.: A blind color image watermarking based on DC component in the spatial domain. Optik **124**, 255–6260 (2013)
34. Pareek, N., Patidar, V., Sud, K.: Image encryption using chaotic logistic map. Image Vis. Comput. **24**, 926–934 (2006)
35. Chen, G., Mao, M., Chui, C.: A symmetric image encryption based on 3D chaotic map. Chaos Solut. Fractals **21**, 749–761 (2004)
36. Shabir, A.P., Javaid, A.S., Bhat, G.M.: Hiding in encrypted images: a three tier security data hiding system. Multidimens. Syst. Signal Process. **28**(2), 549–572 (2017)
37. Parah, S.A., Sheikh, J.A., Hafiz, A.M., Bhat, G.M.: A secure and robust information hiding technique for covert communication. Int. J. Electron. **102**, 1253–1266 (2014)
38. Parah, S.A., Javaid, A.S., Nazir, L., Farhana, A., Bhat, G.M.: Information hiding in medical images: a robust medical image watermarking system for E-Healthcare. Multimed. Tools Appl. **76**(8), 10599–10633 (2017)
39. Nidhi, S.: A new image encryption method using chirikov and logistic map. Int. J. Comput. Appl. **59**, 2123–2129 (2013)
40. Patra, J.C., Phua, J.E., Bornand, C.: A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. Digit. Signal Proc. **20**(6), 1597–1611 (2010)
41. Chengqing, L., Tao, X., Qi, L., Ge, C.: Cryptanalyzing image encryption using chaotic logistic map. Nonlinear Dyn. **78**, 1545–1551 (2014)
42. Eric, Y.X., Chengqing, L., Simin, Y., Jinhu, L.: On the cryptanalysis of Fridrich's chaotic image encryption scheme. Sig. Process. **132**, 150–154 (2017)
43. Chengqing, L., Dongdong, L.: Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. IEEE Multimed. **24**(3), 64–71 (2017)
44. Chengqing, L., Shujun, L., Muhammad, A., Juana, N., Gonzalo, A., Guanrong, Chen: On the security defects of an image encryption scheme. Image Vis. Comput. **27**, 1371–1381 (2009)