A Security Enhanced Robust Steganography Algorithm for Data Hiding

Siddharth Singh [1] and Tanveer J. Siddiqui[2]
[1&2] Department of Electronics and Communication, University of Allahabad
Allahabad, India

Abstract

In this paper, a new robust steganography algorithm based on discrete cosine transform (DCT), Arnold transform and chaotic system is proposed. The chaotic system is used to generate a random sequence to be used for spreading data in the middle frequency band DCT coefficient of the cover image. The security is further enhanced by scrambling the secret data using Arnold Cat map before embedding. The recovery process is blind. A series of experiments is conducted to prove the security and robustness of the proposed algorithm. The experimental results demonstrate that the proposed algorithm achieves higher security and robustness against JPEG compression, addition of noise, low pass filtering and cropping attacks as compared to other existing algorithms for data hiding in the DCT domain.

Keywords: *Steganography, Data hiding, DCT, Chaotic sequence, Arnold transform.*

1. Introduction

With the advancement of high speed computer networks, multimedia storage and transmission technology huge amount of information is being communicated in digital form. There is a continuous threat to copyright, ownership and integrity of digital data. This has made information security an emerging area of research. Steganography is an art of covert communication in which a secret message is communicated by hiding it in a cover file, so that the very existence of the secret message is not detectable. The cover file can be image, audio or video; the most commonly being the image files.

This paper presents a new secure and robust steganography method for data hiding in DCT domain. Both the cover and the data being hidden is an image. The security and robustness is achieved using Arnold cat map and chaotic sequence. Most of the work in information hiding in steganography has been done in invisible watermarking domain. Few earlier reported work involving chaotic sequences and Arnold transform include [1-3].

Kung et al. [1] uses chaotic sequence for scrambling the watermark while [2] uses both chaotic map and Arnold transform for encrypting watermark. This is unlike the proposed work which uses two pseudo random sequences, one for 0 and another for 1, generated by logistic map to spread data in the middle band of DCT coefficients of the cover image. In order to enhance the security further, the secret image is scrambled using Arnold cat map before embedding. Sequences produced by logistic map exhibit random behavior and are quite sensitive to original value, i.e., sequences generated using two different initial sequences are highly uncorrelated which is desirable for spreading. Use of Arnold transform increases the security and makes the proposed algorithm more robust against geometrical transformation like cropping.

We evaluate and compare the performance of the proposed algorithm in terms of standard evaluation measures: Bit error rate (BER), normalized correlation (NC), and peak signal to noise ratio (PSNR). The simulation has been carried out on three standard cover images (Lena, Girl and Tank images) and two images (secret data). The experimental results demonstrate that the proposed algorithm achieves higher security and robustness against JPEG compression, addition of different noise (Gaussian noise, salt and pepper and multiplicative speckle noise), low pass filtering and cropping as compared to other existing algorithm for data hiding using DCT coefficients.

The rest of the paper is organized as follows. Section 2 briefly reviews existing literature and introduces background concepts. In Section 3, the proposed method is discussed. In section 4, experimental results are given. Finally, conclusions are drawn in Section 5.

2. **Literature Review and Background**

2.1 Literature Review

Based on the embedding domain, the existing image steganography methods can be classified into spatial domain and transform domain methods. Spatial domain methods embed the secret data directly embedded into pixels of the cover image. The two most widely used spatial domain steganography techniques are the Least Significant Bit (LSB) and Bit Plane Complexity Steganography (BPCS) technique [4-7]. In LSB technique, the LSB of cover image are replaced by embedded bits. In BPCS the cover image is divided into blocks and classified into information and noisy blocks, the secret data is hidden into noisy blocks. These techniques are computationally simple and straightforward but are more fragile to external attacks and, therefore, less robust. Transform domain methods, also known as frequency domain, first transform the cover image into a set of frequency domain coefficients using Fourier transform, Discrete Cosine Transform (DCT) or wavelet transform. The secret data is then embedded in transformed coefficients. Transform domain methods require more computations but are robust against common image processing operations such as existing image compression standards (JPEG, MPEG, JPEG2000, etc.), low-pass filtering, cropping, and addition of noise [9]. Steganography using DFT requires encoding of both magnitude and phase information of image and is not compatible with the international data compression standards such as JPEG and MPEG whereas DWT is not popular for JPEG and MPEG compression of image/video files. Due to relatively low computational complexity and compatibility with the international data compression standards like JPEG and MPEG, DCT domain steganography technique is widely used. There a number of publicly available steganography tools that embed data by modifying DCT coefficients including Jsteg [10], Outguess [11] and F5 [12]. Both Jsteg and F5 embed the data into the quantized DCT (Discrete Cosine Transform) coefficients of JPEG image. F5 permutes the DCT coefficients before embedding and employs matrix embedding. An improvement of coding method used in F5 is proposed by Fan et al. [13]. Outguess also embeds data by flipping LSBs of DCT coefficient, but it spreads out changes by selecting coefficients with the user-selected password [14]. An extensive survey of digital image steganography can be found in [15].

2.2 Background

2.2.1 Discrete Cosine Transform

The DCT is closely related to DFT, but offers a high energy compaction property in comparison with DFT for natural images [16]. It is a real domain transform which represents an image as coefficient of different frequencies of cosine which is basis vector for this transform. Two-dimensional discrete cosine transformation and its inverse transform for N × N image are defined as follows:

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)Cos[\frac{\Pi(2x+1)u}{2N}]Cos[\frac{\Pi(2y+1)v}{2N}] \quad (1)$$

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)c(u,v)Cos[\frac{\Pi(2x+1)u}{2N}]Cos[\frac{\Pi(2y+1)v}{2N}] \quad (2)$$

Where, $x, y = 0, 1, 2\ldots\ldots N-1$

$$\alpha(u) = \sqrt{\frac{1}{N}} \qquad u=0;$$

$$\alpha(u) = \sqrt{\frac{2}{N}} \qquad u=1,2\ldots\ldots N-1$$

We find $\alpha(v)$ from $\alpha(u)$ by substituting u as v, where u, v $\epsilon\{0,1,2, \ldots.7\}$. $C(u,v)$ is the DCT coefficient of 8×8 block of image, $f(x,y)$ is intensity of $(i,j)^{th}$ pixel. in eq.(5). 64 DCT coefficients are scanned in Zig-Zag manner. It contains 6 low frequency coefficients (f_l), 22 mid – frequency coefficients (f_m) and 36 high frequency coefficients (f_h) [3]. The mid-frequency region, shown by shaded regions in fig. 1, is a popular choice for data embedding due to their moderate variance property.

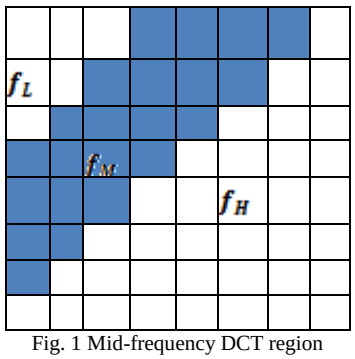


Fig. 1 Mid-frequency DCT region

2.2.2 Arnold Transform

Arnold transform, also known as Arnold's cat map, is a type of image scrambling methods. The transformation shifts pixel position from (x, y) to (x', y') without changing

its gray value. It is cyclic, i.e., the original image repeats itself after certain number of iteration. Given N×N square image, the Arnold transform is defined as follows [8]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N) \quad (3)$$

Where, (x,y) $\in$ {0,1,2,3….N-1} are pixel coordinates of the original image, (x',y') is the transformed position of (x,y) and mod is modulo operation.

The encryption quality of the transform is measured in terms of scrambling degree. Table 1 shows the relation of scrambling time and degree of watermark image of size 64×64. As the scrambling degree is high after 20 iterations, this value is used for scrambling image.

Table 1: Variation of scrambling degree with number of iterations

Number of iterations	1	5	9	20	36
scrambling degree	0.0569	0.4269	0.4192	0.4647	0.4461

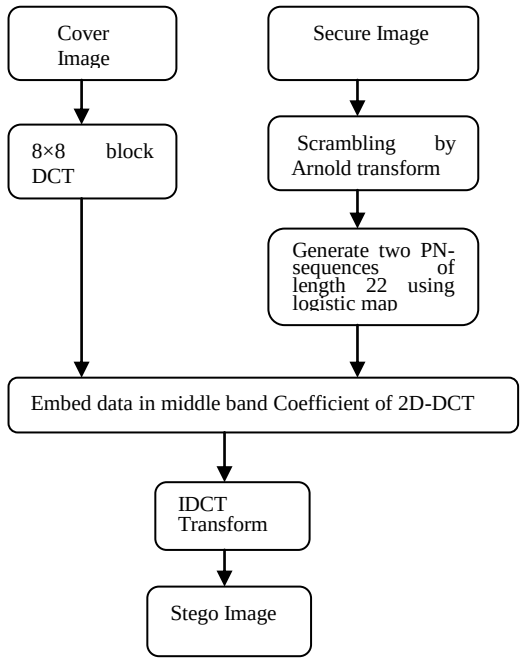
2.2.3 Chaotic Sequence

The most important feature of chaotic system is its sensitivity to initial conditions. Two very close initial conditions may result in drastically different long-term behavior of the system. Due to this sensitivity, a chaotic system exhibits random behavior, even though it is deterministic. Hence, a chaotic map can be used to generate a large number of non-periodic, noise-like yet deterministic and reproducible sequences [17]. A direct application of chaos theory in steganography is to use it for generating pseudo random sequence to spread data. Various non-linear dynamic systems are used to generate the chaotic sequence, e.g., logistic map and tent map [18] [19]. In this work, we use logistic map to generate random sequences. The recurrence relation for the logistic map is:

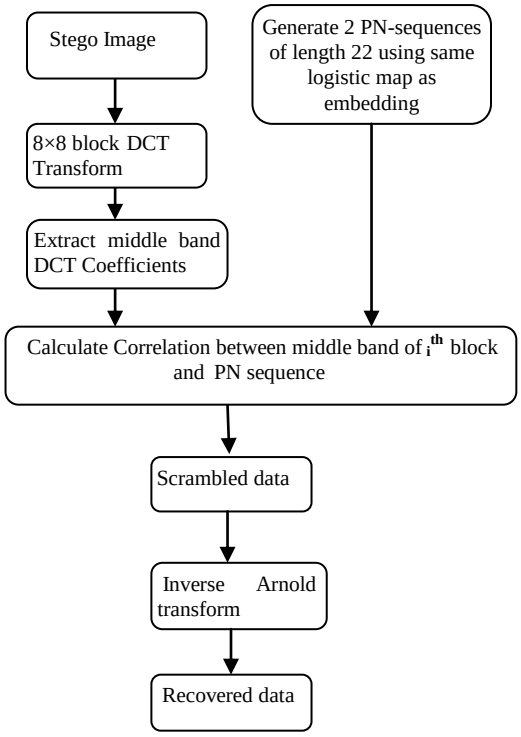
$$x_{k+1} = r \cdot x_k (1 - x_k), \; 0 < x < 1 \quad (4)$$

$$x_{k+1} = (1 - 2x_k^2), \; -1 < x < 1 \quad (5)$$

where $0 < r \leq 4$ is bifurcation parameter. Research on chaos dynamic system shows that when $3.569945 < r \leq 4$, the logistic map is in chaotic state [17].



(a) Embedding Process



(b) Recovery Process

Fig. 2 Block diagram of the proposed steganography method

3. The Proposed Method

Fig. 2 shows the embedding and recovery steps of the data hiding algorithm. For embedding, the cover image is first divided into 8×8 sub blocks and transformed using DCT. To increase the security further, the data (image) is scrambled using Arnold transform and then embedded in the middle frequency band DCT coefficients of the image blocks. The spreading is done using two chaotic sequences, one for '0' and another for '1, each of length similar to middle frequency DCT band. The security is increased by using three different keys, one key for scrambling and two keys for generating chaotic sequences. Finally, the stego image is obtained by taking inverse discrete cosine transform (IDCT). Recovery is an inverse process of embedding which finds correlation between middle frequency band DCT coefficients and the chaotic sequences for 0 and 1 bit. The data is then extracted by applying inverse Arnold transform same number of times as applied during embedding process. The secret data used for embedding is in the binary image format. The steps in the embedding and recovery process are listed below:

3.1 Embedding Process

1. Read Cover and logo image.
2. Apply Arnold transform on logo image 20 times (encryption key =20).
3. Generate two random sequences, s^0 and $s^{1,}$ of length 22 (for 22 mid-band DCT coefficients) using logistic map. The bifurcation parameter and the initial value of the logistic map define the secret keys. The resulting sequence is converted into binary sequence using a threshold(t = 0.5) as follows:

$$p_i^k = \begin{cases} 1, if\ s_i^k \geq t \\ -1, if\ s_i^k < t \end{cases}, \quad k = 0\ or\ 1 \qquad (6)$$

4. Transform the original image using 8×8 block 2D-DCT.
5. Hide the i^{th} scrambled watermark bit, by modulating the i^{th} DCT block of the host using following equation (for 0 and 1 bit):

$$f_S(u,v) = \begin{cases} f(u,v) + \alpha * p^k(u,v), & \text{if } u,v \in f_M \\ f(u,v), & \text{if } u,v \notin f_M \end{cases} \qquad (7)$$

Where, f_m is the mid-band frequency region, n is message length, α is the gain factor used to specify the strength of the embedded data. The value of the gain factor is set to 6 experimentally. p^k is the appropriate pseudo random noise sequence depending on message bit (0 or 1); f(u,v) represents the 8×8 DCT block of the cover image and $f_s(u,v)$ represents corresponding stego image block.

6. Take the inverse transform of each of the stego blocks, $f_s(u, v)$, using 8x8 block inverse 2D-DCT to get the final stego image $f_s(x, y)$.

3.2 Recovery Process

The recovery procedure is based on correlation between the middle frequency band DCT coefficients of the image and corresponding random sequences. The steps involved in recovery are:

1. Read stego image.
2. Generate two pseudo-random (PN) sequences using logistic map
3. Transform the stego image using 8×8 block 2D-DCT.
4. Extract the middle band DCT coefficients in C_i.
5. For i=1 to N

(a) Calculate the correlation between the mid-band DCT coefficients of block and the PN-sequences for 0 and 1.

(b) Extract the i^{th} scrambled data bit, b_i using the following expression:

$$b_i = \begin{cases} 0, \text{ if } corr(p^0, C_i) > corr(p^1, C_i) \\ 1, \text{ otherwise} \end{cases} \qquad (8)$$

Where, corr (p^0, C_i) is the correlation between scrambled extracted coefficient of i^{th} block and PN sequence generated for bit '0'. corr (p^1, C_i) is the correlation between scrambled extracted coefficient of i^{th} block and PN sequence generated for bit '1'.

6. Extract data by applying inverse Arnold transformation on the scrambled data with the key used during embedding process.

4. Experiments and Results

We have conducted a series of experiments using three different cover images and two logo images, hence forth called M1 and M2, to test the performance of the proposed algorithm. The cover images are 512 × 512 gray scale Lena, Girl and Tank image and the two logo images are 64 × 64, 8-bit binary logo image(M1) and a text image (M2) as shown in fig. 3. The proposed algorithm uses three kinds of keys- one for encryption and the other two for generating chaotic sequences. The host image is first divided into 4096 blocks of size 8 × 8. The logo is scrambled using Arnold transform. The logistic map is used for generating two random sequences using initial value (x_0) and bifurcation parameter (r) as its secret keys. The random sequence is converted into binary sequence

and logo is embedded by employing the method described in section 3. Fig. 3 shows stego image after embedding M1 and M2 in Lena image. In order to evaluate imperceptibility of the algorithm Peak signal to Noise Ratio (PSNR) between original and stego image is computed and results are listed in Table 1. The PSNR of an M×N gray-scale image is defined as:

$$PSNR = 10\log_{10}\left(\frac{L^2}{MSE}\right) \quad (9)$$

Where, L is peak signal value of the image and the Mean Square Error (MSE) between the original and the stego image is calculated as follows:

$$MSE = \frac{1}{MN}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}\left(f(i,j) - f'(i,j)^2\right)\right] \quad (10)$$

In order to compare the extracted and original logo, bit error rate and normalized correlation is calculated and listed in table 2 along with PSNR for different gain factor. The Bit Error Rate (BER) is the ratio of the number of erroneous detected bits to the total number of watermark bits. The normalized cross correlation (NC) coefficient is used to measure the similarity between the original (M) and the extracted data(M'). It is defined as follows:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} M(i,j)\times M(i,j)}{\sqrt{\sum_{i=1}^{M} M(i,j)^2 \sum_{j=1}^{N} M'(i,j)^2}} \quad (11)$$

Table 2. PSNR, BER and NC for different cover and secret images for different gain factor

Image	Gain factor(α)	PSNR(dB)	BER	NC
Lena	4	40.74	0.044	0.9253
	5	38.67	0.0320	0.9370
	6	37.10	0.0225	0.9475
Girl	4	40.74	0.0288	0.9399
	5	38.67	0.0161	0.9523
	6	37.10	0.0100	0.9591
Tank	4	40.74	0.054	0.9126
	5	38.67	0.0295	0.9394
	6	37.10	0.0171	0.9523

(a) after embedding M1

(b) after embedding M2

(c) Original and recovered Images

Fig. 3

Table 2 shows that the PSNR values are greater than 37 dB for all cover images for different gain factors. This suggests that the proposed algorithm is good in terms of invisibility of the embedded data. In the following, the results of evaluating the proposed data hiding algorithm for robustness against a range of common attacks are presented.

(a) Lena (PSNR=35.03dB)

(b) Girl (PSNR=32.20dB)

(c) Recovered watermarks Lena (NC=0.9562), Girl (NC=0.9765)

Fig. 4 Stego image under JPEG compression (Q-60)

4.1 JPEG Compression

JPEG compression can be serious form of distortion for data hiding, so we compressed stego images with different quality factors (90, 80, 70, 60 and 50). Fig. 4 shows compressed stego Lena and Girl image for quality factor 60 along with the extracted images. Figure 5 compares the BERs in JPEG compression attack with the PN sequence based algorithm [20] with different quality factors and cover images. The normalized correlation (NC) and BER of the compressed images are compared to results from

[20] in Table 3 for M2. Form Table 3, it can be seen that the minimum and maximum BER, for Lena image using M1 is 0.022 and 0.1511 for quality factors 90 and 50 respectively. It means more than 84% of the hidden data was recovered without any error in case of maximum BER. It can be seen from Table 3 that the proposed algorithm is more robust than [20] against JPEG compression and logo can be well detected for quality factor upto 50.

Table 3: Robustness of the proposed algorithm in the presence of JPEG compression attack with different quality factor

Image	Quality factor	M1		M2		PN Sequence based method [20]	
		NC	BER	NC	BER	NC	BER
Lena	90	0.9478	0.0222	.9845	0.0232	0.9626	0.0654
	80	0.9420	0.0273	.9804	0.0305	0.9624	0.0659
	70	0.9295	0.0388	.9748	0.0422	0.9610	0.0684
	60	0.8981	0.0674	.9562	0.0737	0.9490	0.0889
	50	0.8087	0.1511	.9086	0.1533	0.9285	0.1239
Girl	90	0.9583	0.0107	.9926	0.009	0.9724	0.0486
	80	0.9577	0.0122	.9908	0.0122	0.9718	0.0496
	70	0.9499	0.0188	.9869	0.0192	0.9686	0.0552
	60	0.9278	0.0405	.9765	0.0884	0.9623	0.0662
	50	0.8717	0.0935	.9471	0.0884	0.9551	0.0786
Tank	90	0.9496	0.0195	.9864	0.0200	0.9614	0.0676
	80	0.9497	0.0215	.9855	0.0215	0.9575	0.0742
	70	0.9354	0.0322	.9785	0.0322	0.9557	0.0774
	60	0.9181	0.0518	.9656	0.0847	0.9482	0.0901
	50	0.8852	0.0842	.9491	0.0847	0.9390	0.1057

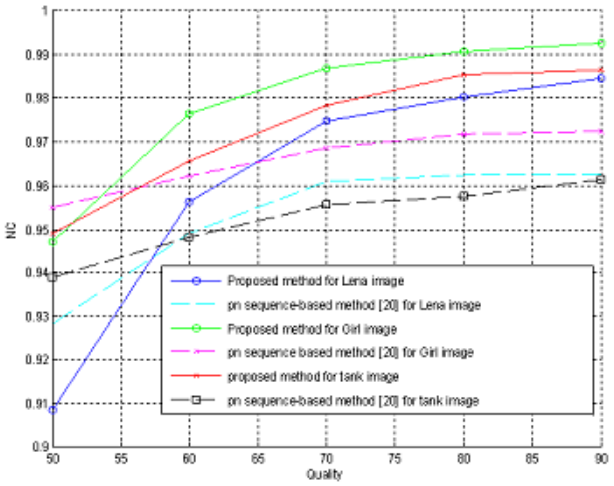


Fig. 5. BER in recovered image (M2) under JPEG compression using proposed algorithm and pn sequence based algorithm [20]

Table 4: NC and BER of extracted images for a low pass filtering with different Gaussian variance

Image	Gaussian variance(σ)	binary logo image		text pattern image	
		NC	BER	NC	BER
Lena	0.5	0.9388	0.0310	0.9792	0.0330
	1.0	0.8807	0.0881	0.9570	0.0708
Girl	0.5	0.9537	0.0149	0.9897	0.0146
	1.0	0.8956	0.0752	0.9683	0.0522
Tank	0.5	0.9835	0.0256	0.9837	0.0247
	1.0	0.8717	0.1023	0.9579	0.0710

4.2 Low-pass Filtering

Robustness of the proposed algorithm is evaluated against Gaussian low-pass filtering attack. Fig. 6 shows stego Lena and girl image after facing Gaussian filter attack with window size of 3×3. Table 4 presents the bit error rate and normalized correlation in the presence of Gaussian filter with filter size of 3×3 and variance of 0.5 and 1.0 for the three cover images and the two logo images. A Gaussian low–pass filtering attack does not affect the robustness of hidden data by a considerable amount. The data hiding algorithm does not fail under the low pass filter with different window size 5×5, 8×8.

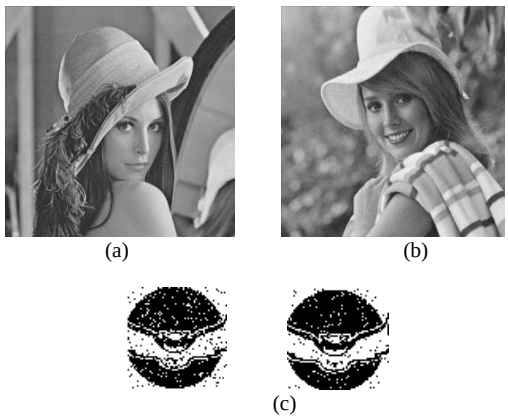


Fig. 6. Stego image after low-pass filtering with window size 3×3 (a) Lena, (b) Girl and (c) Recovered logo (M1) from Lena(NC=0.9570) & Girl(NC=0.9683) images

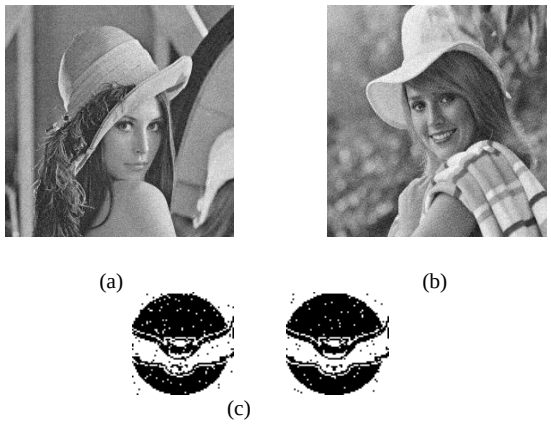
4.3 Addition of Gaussian noise

The results of evaluation of the proposed algorithm in the presence of Gaussian noise is presented in table 5. The mean of the additive Gaussian noise is zero and variance is varied between 0.0001 and 0.001. The extracted image M1 obtained using the proposed method for Lena and Girl images are shown in fig. 7 for variance .001. The stego image quality is degraded but the recovered image is easily

detected. From table 5, it can be seen that the NC between extracted and original image is well above 90 in all the cases for different variance.

Table 5: Performance metrics under Gaussian noise attack

Image	Variance	M1		M2	
		NC	BER	NC	BER
Lena	0.0001	0.9467	0.0232	0.9843	0.0242
	0.0003	0.9354	0.0244	0.9837	0.0247
	0.0005	0.9421	0.0269	0.9826	0.0271
	0.0007	0.9397	0.0295	0.9797	0.0322
	0.0009	0.9391	0.0300	0.9786	0.0342
	0.001	0.9334	0.0344	0.9777	0.0332
Girl	0.0001	0.9577	0.0166	0.9926	0.0095
	0.0003	0.9553	0.0183	0.9918	0.0122
	0.0005	0.9553	0.0205	0.9891	0.0151
	0.0007	0.9499	0.0244	0.9872	0.0191
	0.0009	0.9485	0.0205	0.9854	0.0217
	0.001	0.9442	0.0244	0.9837	0.0247
Tank	0.0001	0.9502	0.0190	0.9876	0.0178
	0.0003	0.9467	0.0227	0.9851	0.0222
	0.0005	0.9449	0.0242	0.9829	0.0261
	0.0007	0.9402	0.0291	0.9808	0.0298
	0.0009	0.9345	0.0337	0.9804	0.0305
	0.001	0.9321	0.0364	0.9794	0.0327



(a) (b)

(c)

Fig. 7. Stego image using Gaussian noise with variance 0.001;(a) Lena, (b) Girl and (c) Recovered image M1 from Lena(NC=0.9777) & Girl (NC=0.9837)images.

We evaluated the proposed algorithm in the presence of the salt and pepper noise and the multiplicative speckle noise and listed the results in table 6 and table 7. Fig. 8 compares the BER between the original and the extracted binary logo in the proposed steganography method under Salt and Pepper and Speckle noise with different variance. From the obtained results, it can be seen that the proposed algorithm is more robust against the addition of noise (Gaussian noise, salt & pepper and multiplicative speckle noise) attack.

Table 6: Performance metrics with addition of salt and pepper noise attack

Image	Noise density	Binary logo image (M1)		Text pattern image (M2)	
		NC	BER	NC	BER
Lena	0.001	0.9405	0.0288	0.9815	0.0286
	0.003	0.9274	0.0408	0.9751	0.0398
	0.005	0.9207	0.0479	0.9686	0.0510
	0.007	0.9106	0.0596	0.9606	0.0647
	0.01	0.8967	0.0713	0.9555	0.0740
	0.02	0.8368	0.1284	0.9262	0.1248
Girl	0.001	0.9559	0.0139	0.9890	0.0154
	0.003	0.9431	0.0244	0.9840	0.0242
	0.005	0.9343	0.0349	0.9766	0.0376
	0.007	0.9142	0.0552	0.9710	0.0479
	0.01	0.8974	0.0703	0.9595	0.0681
	0.02	0.8572	0.1143	0.9310	0.1147
Tank	0.001	0.9477	0.0212	0.9843	0.0237
	0.003	0.9352	0.0334	0.9766	0.0371
	0.005	0.9243	0.0444	0.9720	0.0466
	0.007	0.9030	0.0654	0.9662	0.0552
	0.01	0.8968	0.0735	0.9515	0.0803
	0.02	0.8409	0.1260	0.9256	0.1216

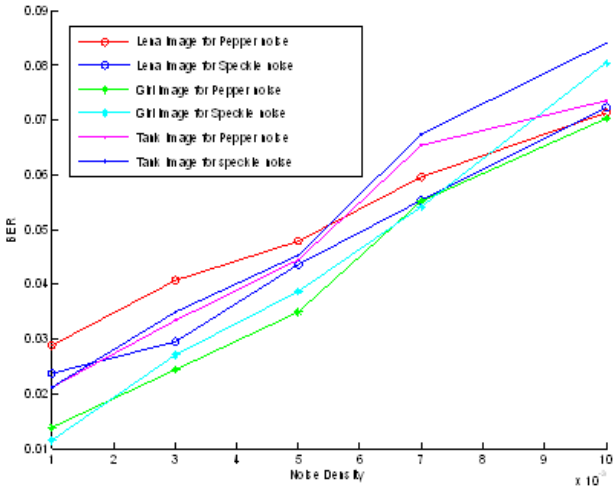


Fig. 8 BERs in salt & pepper noise and multiplicative speckle noise attack

Table 7: Performance metrics with addition of multiplicative speckle noise attack

Image	Noise density	Binary logo image (M1)		Text pattern image (M2)	
		NC	BER	NC	BER
Lena	0.001	0.9461	0.0237	0.9830	0.0259
	0.003	0.9386	0.0295	0.9794	0.0327
	0.005	0. 9257	0.0437	0.9722	0.0452
	0.007	0.9129	0.0554	0.9684	0.0513
	0.01	0.8981	0.0723	0.9558	0.0735
Girl	0.001	0.9580	0.0115	0.9908	0.0122
	0.003	0.9402	0.0271	0.9868	0.0193
	0.005	0.9298	0.0386	0.9774	0.0356
	0.007	0.9118	0.0542	0 9659	0.0557
	0.01	0.8858	0.0806	0.9522	0.0791
Tank	0.001	0.9477	0.0212	0.9851	0.0222
	0.003	0.9356	0.0349	0.9784	0.0344
	0.005	0.9239	0.0454	0.9703	0.0486
	0.007	0.8991	0.0674	0.9599	0.0664
	0.01	0.8853	0.0842	0.9480	0.0872

4.4 Cropping operation

Images M1 and M2 are tested for geometric attack of cropping by varying cropping percentage from 6.25% to 25% and the results are compared with the method [20].The result are listed in table 8. The extracted images, M1 and M2, after cropping 25% middle portion of Lena and Girl image are shown in fig. 9. From the obtained results, it can be clearly inferred that the proposed algorithm exhibits better robustness than [20] against cropping operation. This is due to pretreatment by Arnold transform.

Fig. 9. Recovered images M1 and M2 after cropping 25% middle portion: Lena(NC=0.9721) & Girl (NC=0.9768) images.

Table 8: Performance metrics with cropping operation

Image	Cropping	binary logo imag (M1)		text pattern image (M2)		PN Sequence based Algo.[20]	
		NC	BER	NC	BER	NC	BER
Lena	Upper right 6.25%	0.9163	0.0574	0.9811	0.0293	0.9629	0.0649
	Upper right 25%	0.8417	0.1580	0.9730	0.0461	0.9565	0.0771
	middle 25%	0.8390	0.1567	0.9721	0.0479	0.9518	0.0869
Girl	Upper right 6.25%	0.9269	0.0452	0.9897	0.0142	0.9723	0.0488
	Upper right 25%	0.8503	0.1475	0.9809	0.0322	0.9625	0.0667
	middle 25%	0.8437	0.1499	0.9768	0.0396	0.9542	0.0828
Tank	Upper right 6.25%	0.9205	0.0520	0.9850	0.0225	0.9634	0.0642
	Upper right 25%	0.8461	0.1526	0.9772	0.0388	0.9564	0.0771
	middle 25%	0.8403	0.1533	0.9737	0.0452	0.9472	0.0947

6. Conclusions

This paper proposed a new steganography technique in DCT domain. The proposed algorithm uses Arnold transform to scramble the secret image and logistic map to generate random sequence. This increases security level. The proposed algorithm is based on blind data recovery. The experimental results shows that the proposed algorithm achieves multilayer security and robustness against JPEG compression, addition of noise (Gaussian noise, salt & pepper and multiplicative speckle noise), low pass filtering and cropping operation as compared to other existing DCT domain data hiding algorithm. Performance evaluation for robustness and imperceptibility of the proposed algorithm has been done using bit error rate (BER), normalized correlation (NC), and peak signal to noise ratio (PSNR) for different logo and cover images. The observed results demonstrate that this algorithm also induces low distortion in the cover image. The main features of the algorithm are imperceptibility, robustness, security and blind watermark recovery. Hybrid transform domain techniques can be tried to make the algorithm more robust.

References

[1] C M Kung, S T Chao, Y C Tu, Y H Yan, and C H Kung, A robust watermarking and image authentication scheme used for digital content application, J. Multimedia 4, 112-119(2009).

[2] Jianhu Song and Yong Zhu, A Digital Watermarking Method by Double Encryption Based on Arnold and Chaos in DCT domain, Applied Mechanics and Materials, 65, 104-107 (2011).

[3] Siddharth Singh, Tanveer J. Siddiqui, Rajiv Singh and Harsh V. Singh, DCT-domain Robust Data Hiding Using Chaotic Sequence, in Proceedings of International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT), AMU Aligarh, 300-303(2011).

[4] Han-ling ZHANG, Xiao-yan ZHANG and LI Li-jun. A New BPCS Steganography Against Statistical Analysis Journal of Hunan University (Natural Sciences) 34, No.4, 68-72 (2007).

[5] Yu Lifang, Zhao Yao and Ni Rongrong, Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm. EURASIP Journal on Advances in Signal Processing 2010, DOI:10.1155/2010/876946 (2010).

[6] R. M. Shreelekshmi, C.E. Wilscy and V. Madhavan, Cover Image Preprocessing for More Reliable LSB Replacement Steganography. Proc. Of International Conf. on Signal Acquisition and Processing, 153-156 (2010).

[7] Chan C K and Chen L M, Hiding data in images by simple LSB substitution", Pattern Recognition 37, 469–474 (2004).

[8] A. Westfeld and A. Pfitzmann, Attacks on steganographic systems, Lecture Notes in Computer Science, Springer-Verlag, 1768, 61-75 (2000).

[9] Y.L. Guan , J. Jin. An objective comparison between spatial and DCT watermarking schemes for MPEG video, Proceedings International Conference on Information Technology: Coding and Computing, 207- 211(2001).

[10] D. Upham, JPEG - Jsteg. [Online]. Available: Http://zooid.org/~paul/crypto/jsteg/

[11] N. Provos, Defending against statistical steganalysis. In: Proceedings of tenth USENIX security symposium'01, (Washington DC), 323–335(2001).

[12] A. Westfeld, F5-a Steganographic algorithm: High capacity despite better Steganlysis. Lecture Notes in Computer Science 2137, Springer-Verlag, Berlin, 289-302 (2001).

[13] Li Fan, Tiegang Gao, Qunting Yang and Yanjun Cao, An extended matrix encoding algorithm for steganography of high embedding efficiency Original Research Article, Computers & Electrical Engineering 37, No. 6, 973-981(2011).

[14] Neils Provos and Peter Honeyman, Detecting Steganographic Content on the Internet", CITI Technical Report 01-11(2001).

[15] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, Digital image Steganography: Survey and analysis of current methods, Review Article, Signal Processing 90, No. 3, 727-752(2010).

[16] Harsh.V. Singh, Mohan Rai Suresh, Anand Mohan and Surya P. Singh, Robust copyright marking using Weibull distribution, Computers & Electrical Engineering 37, 714-728(2011).

[17] Hongxia Wang, Public Watermarking Based on Chaotic Map, IECE Trans. Fundamentals E87-A, No. 8, 2045-2047 (2004)

[18] Hai Wang and Jiandong Hu, Logistic-Map chaotic spread spectrum sequence, ACTA Electronica sinica 25, No. 1, 19-23(1997).

[19] M. Jessa, The period of sequences generated by tent- like maps, IEEE trans.Circuits syst.I, Fundam.Theory appl. 49 (1), 84-88 (2002).

[20] Siddharth Singh, Tanveer J Siddiqui and Harsh Vikram Singh, DCT Based Digital Data Hiding in Image Cover, International Journal of System Simulation 5, No.1, 45-49 (2011).

Siddharth Singh obtained his B.Tech degree from Purvanchal University, Jaunpur (India) and M.Tech in Electronics and Communication Engineering from Integral University, Lucknow in year 2009.Currently, he is pursuing his Ph.D from University of Allahabad, Allahabad. His areas of interest are information security, steganography and digital image processing.

Dr.Tanveer J Siddiqui, M.Sc., Ph.D**.,** currently, Assistant professor with the Department of Electronics and Communication at University of Allahabad, Allahabad. She has 13 years of experience in teaching and research. Her area of research includes Natural Language Processing and Information Retrieval/Processing. She has got about 25 publications in refereed Journals and conferences. She has co-authored/edited five books.