Hindawi
Journal of Healthcare Engineering
Volume 2022, Article ID 7745132, 14 pages
https://doi.org/10.1155/2022/7745132

Research Article

Multi-Chaos-Based Lightweight Image Encryption-Compression for Secure Occupancy Monitoring

Yazeed Yasin Ghadi,[1] **Suliman A. Alsuhibany**,[2] **Jawad Ahmad**,[3] **Harish Kumar**,[4] **Wadii Boulila**,[5,6] **Mohammed Alsaedi**,[7] **Khyber Khan**,[8] **and Shahzad A. Bhatti**[9]

[1]*Department of Computer Science and Software Engineering, Al Ain University, Abu Dhabi 15551, UAE*
[2]*Department of Computer Science, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia*
[3]*School of Computing, Edinburgh Napier University, Edinburgh, UK*
[4]*Department of Computer Science, College of Computer Science, King Khalid University, Abha, Saudi Arabia*
[5]*Robotics and Internet of Things Lab, Prince Sultan University, Riyadh, Saudi Arabia*
[6]*RIADI Laboratory, University of Manouba, Manouba, Tunisia*
[7]*College of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia*
[8]*Department of Computer Science, Khurasan University, Jalalabad, Afghanistan*
[9]*Department of Electrical and Electronic Engineering, University of Strathclyde, Glasgow, UK*

Correspondence should be addressed to Khyber Khan; khyber.khan.khurasan@gmail.com

Received 12 March 2022; Revised 2 April 2022; Accepted 7 April 2022; Published 8 November 2022

Academic Editor: Muhammad Asghar Khan

With the advancement of camera and wireless technologies, surveillance camera-based occupancy has received ample attention from the research community. However, camera-based occupancy monitoring and wireless channels, especially Wi-Fi hotspot, pose serious privacy concerns and cybersecurity threats. Eavesdroppers can easily access confidential multimedia information and the privacy of individuals can be compromised. As a solution, novel encryption techniques for the multimedia data concealing have been proposed by the cryptographers. Due to the bandwidth limitations and computational complexity, traditional encryption methods are not applicable to multimedia data. In traditional encryption methods such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), once multimedia data are compressed during encryption, correct decryption is a challenging task. In order to utilize the available bandwidth in an efficient way, a novel secure video occupancy monitoring method in conjunction with encryption-compression has been developed and reported in this paper. The interesting properties of Chebyshev map, intertwining map, logistic map, and orthogonal matrix are exploited during block permutation, substitution, and diffusion processes, respectively. Real-time simulation and performance results of the proposed system show that the proposed scheme is highly sensitive to the initial seed parameters. In comparison to other traditional schemes, the proposed encryption system is secure, efficient, and robust for data encryption. Security parameters such as correlation coefficient, entropy, contrast, energy, and higher key space prove the robustness and efficiency of the proposed solution.

1. Introduction

A fully automatic human occupancy information system has various commercial applications [1], for example, passenger counting, identifying hourly office patterns, and counting shopping center footfall. Researchers have proposed various occupancy measurement solutions through various sensors over the last two decades [1]. These sensors include camera, passive infrared (IR), ultrasonic, CO_2, Wi-Fi, and radio frequency (RF) identifiers [2]. However, it is reported that camera-based human occupancy techniques are more accurate when compared to other sensor-based methods. The biggest issue with the camera-based occupancy is monitoring occupancy with privacy preservation [2, 3]. In such

scenarios, encryption can play a vital role and can hide the information and identity of individuals during the occupancy process [3]. In video encryption, identity of individuals is concealed and only an authorized person who has correct key information can decrypt the original video contents [4].

Images and videos can be encrypted using traditional schemes such AES and DES; however, these schemes are not designed for multimedia data encryption [5–7]. Conventional encryption schemes have some issues such as higher computational complexity as images contain large amount of data and strong correlation among pixels. As a result, traditional encryption schemes fail to satisfy real-time implementation constraints and thus have limited applications in the real-time multimedia applications [8]. To overcome the aforementioned issues, chaotic maps can provide highly secure encryption due to complex dynamics and ergodicity.

Mathews introduced the concept of chaos-based encryption algorithms [9], and since then many algorithms using chaos theory have been proposed [10]. For example, a novel image encryption scheme based on Henon and Ikeda chaotic maps and a lattice model based on Arnold coupled logistic map (ACLM) have been proposed in [11, 12]. In the lattice model, the coupling coefficients are generated from the logistic map that is further employed in diffusion and permutation processes. Moreover, ACLM is employed in key generation and an efficient scheme is presented. Saiyma et al. proposed a novel encryption algorithm using Rubik's cube puzzle and logistic chaotic map for pixel permutation and diffusion [13]. Another encryption scheme that utilizes Rubik's cube puzzle for the permutation of bits and XOR operation for diffusion was proposed in [14].

A key-based block ciphering method was presented in [15] where pixel bytes are encrypted and shuffled using variable block sizes that enhance the diffusion property. Zhao and Ren [16] employed infinite-dimensional hyperchaotic multi-attractor (HCMA) Chen system that was generated by a linear time-delay feedback control for the encryption of digital images. In [17], piecewise linear chaotic map (PLCM) and S-Box transformation are applied on original plaintext image. Furthermore, an XOR operation is applied to the diffused image pixels. Elements for XOR operations were based on mixing of chaotic logistic random sequence. A hybrid chaos-based random stream and blockwise encryption algorithm with a key stretching method for the enhancement of security was presented in [18]. Chai et al. [19] proposed an image compression and encryption scheme by combining a parameter-varying chaotic system, elementary cellular automata (ECA), and block compressive sensing (BCS). Musanna et al. proposed a secure image encryption using multi-chaotic maps and multi-resolution singular value decomposition (MR-SVD) for secure image encryption [20].

In [21], fractional Fourier transform (FRFT), DNA sequencing, and chaos theory have been used for image security. However, there are several issues in DNA-based image encryption [22]. These issues were higher computational complexity and inappropriate implementation. In order to address the drawbacks of DNA-coding-based encryption algorithms, a new technique was introduced in [22] which is based on the integer wavelet transform (IWT) and global bit scrambling (GBS) for image encryption. Previously, video and image encryption schemes have been proposed, but they are either insecure or impractical.

2. Preliminaries

2.1. Chaotic Maps. Any mathematical function that exhibits chaotic behavior is known as chaotic map. A close association between chaos and cryptography has been widely reported in literature since many decades. This close relationship is due to high sensitivity of initial conditions, deterministic dynamics, and attack complexity of chaotic map. Logistic map shown in equation (1) is an example of one-dimensional (1D) chaotic map [23]:

$$Z_{n+1} = \mu Z_n (1 - Z_n), \tag{1}$$

where the initial parameters are

$$\begin{aligned} Z_0 &\in (0, 1), \\ \mu &\in (0, 4). \end{aligned} \tag{2}$$

The bifurcation diagram of logistic map is shown in Figure 1. It is clear from Figure 1 that the logistic map has chaotic behavior for the range $3.57 \le \mu \le 4$. Any variation of μ within this range results in a random output of the logistic map. Range of μ is low and hence an intruder can apply exhaustive key search attack.

The key processes of an image encryption technique are confusion and diffusion. In our proposed scheme, Chebyshev and intertwining chaotic maps are employed in confusion and diffusion processes. Mathematically, Chebyshev map can be defined as [24, 25]

$$T_k(A) = \cos(k \times \arccos(A)), \tag{3}$$

where k is an integer and $A \in [-1, 1]$. It is proposed that $k = 4$ for less computation requirements [25].

The intertwining map can be written as [26]

$$\begin{aligned} X_{n+1} &= (\lambda \times A_1 \times Y_n \times (1 - X_n) + Z_n) \bmod (1), \\ Y_{n+1} &= \left(\frac{\lambda \times A_2 \times Y_n + Z_n}{1 + (X_{n+1})^2} \right) \bmod (1), \\ Z_{n+1} &= \lambda \times (X_{n+1} + Y_{n+1} + A_3) \times \sin(Z_n) \bmod (1), \end{aligned} \tag{4}$$

where X_n, Y_n, and $Z_n \in (0, 1)$, $0 \le \mu \le 3.999$, $|A_1| > 33.5$, $|A_2| > 37.9$, $|A_3| > 35.7$. Key space of intertwining logistic map is $10^{60} \approx 2^{200}$ which reduces the possibility of brute force attack.

2.2. Substitution Box. In symmetric key cryptography, substitution is a nonlinear bijective function. Generally, m bits are given as an input to substitution box (S-Box), and as a result, n bit output is produced [27, 28]. In case of digital images, the bijective function F: $I \longrightarrow S$ maps each image

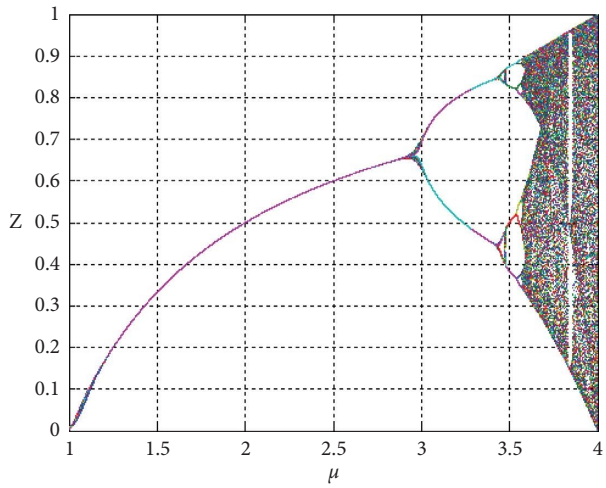


Figure 1: Bifurcation diagram (μ spacing is 0.0005).

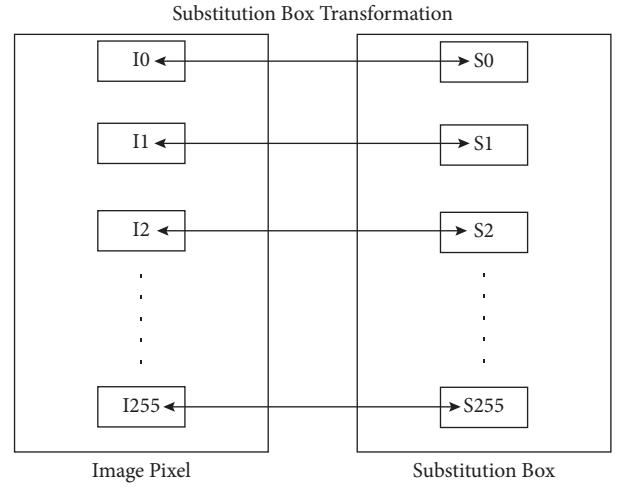


Figure 2: Bijective mapping of substitution box.

pixel I to a unique value S as shown in Figure 2. In many traditional algorithms such as AES and DES, S-Box is the only nonlinear part of ciphertext. In our previous research, it has been highlighted that substitution-only image encryption scheme is highly vulnerable to various types of attacks. Thus, the use of a single S-Box in image encryption algorithms is not a good choice due to weaker security. Instead of a single fixed S-Box, we have used three S-Boxes known as AES S-Box [29], Khan's S-Box [30], and Tayseer's S-Box [31], respectively. Due to higher nonlinearity and good resistance against different attacks, we have selected these S-Boxes in our proposed scheme. These S-Boxes are outlined in Tables 1–3. In the proposed scheme, S-Box is randomly selected using logistic map. The selection of S-Box is based on logistic map which is further explained in later part of the paper.

2.3. Discrete Cosine Transform. Discrete cosine transform (DCT) is a widely used transform for image compression. The DCT and inverse DCT of a plaintext image P is shown in equations (5) and (6), respectively. The DCT $\Delta(u, v)$ of a plaintext image P is written as [32]

$$\Delta(u,v) = \frac{2}{\sqrt{A \times B}} \Gamma(u)\Gamma(v) \sum_{x=0}^{A-1} \sum_{y=0}^{B-1} P(x,y) \cos\left[\frac{(2y+1)u\pi}{2A}\right] \times \cos\left[\frac{(2x+1)v\pi}{2B}\right], \tag{5}$$

$$P(x,y) = \frac{2}{\sqrt{A \times B}} \Gamma(u)\Gamma(v) \sum_{x=0}^{A-1} \sum_{y=0}^{B-1} \Delta(u,v) \cos\left[\frac{(2y+1)u\pi}{2A}\right] \times \cos\left[\frac{(2x+1)v\pi}{2B}\right], \tag{6}$$

where $n \times n$ is the size of image and $\Gamma(u)$ and $\Gamma(v)$ can be written as

$$\Gamma(u) = \Gamma(v) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{for } \frac{u}{v} = 0, \\ 1, & \text{otherwise.} \end{cases} \tag{7}$$

An encryption scheme is divided into two types: (i) full encryption and (ii) partial encryption. In full encryption, the complete image is encrypted, while in partial encryption, only a part of the image is encrypted. Partial encryption effectively reduces computational complexity. When an image is converted to frequency domain such as applying discrete cosine transform (DCT), less attention is given to higher frequency components.

3. The Proposed Real-Time Secure Occupancy Monitoring System

The proposed scheme uses multi-chaos for the encryption of real-time frames obtained from an overhead 2.0 megapixels Logitech camera installed at a height of 1.7 m above the floor in T10 office at Glasgow Caledonian University, United Kingdom. Figure 3 shows real-time frames with one, two, and three occupants, respectively. In order to protect these frames from eavesdropper, a novel lightweight secure occupancy monitoring system is proposed. Flowchart of the proposed encryption-compression system is depicted in Figure 4. It can be seen from Figure 4 that after discrete cosine transformation (DCT), a block starting from direct coefficient (DCT-DC) is selected and then encrypted through confusion (scrambling) and diffusion (substitution) processes. A part of DCT values is selected

Table 1: AES S-Box [29].

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	22	, 121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Table 2: Khan's S-Box [30].

129	148	14	206	208	63	95	219	86	242	69	254	152	215	53	104
47	138	93	200	161	75	230	110	133	103	24	251	106	159	38	167
181	179	31	218	74	155	153	43	249	0	57	52	162	144	243	235
61	108	164	82	117	213	130	99	228	49	39	12	199	189	78	13
116	175	58	180	123	3	194	232	105	22	65	160	5	84	54	102
56	196	66	182	171	212	131	115	183	67	90	64	15	191	60	178
216	204	248	70	73	118	100	146	7	198	207	137	141	94	92	165
202	221	197	127	23	128	85	252	168	233	68	201	174	76	81	124
220	173	170	225	16	62	25	107	145	46	20	41	122	17	192	187
45	244	247	227	156	157	101	214	71	79	222	226	112	139	30	72
210	172	37	253	239	89	119	35	88	147	97	83	154	33	149	11
4	36	50	176	21	224	120	158	184	51	87	9	114	246	231	217
241	42	240	211	229	250	236	125	136	48	190	237	8	98	27	29
203	193	1	205	188	91	245	143	6	177	96	166	80	142	185	40
140	111	113	55	28	195	26	234	209	135	32	186	134	151	126	132
169	223	10	163	34	19	77	150	44	255	2	121	109	59	238	18

Table 3: Tayseer's S-Box [31].

9	47	204	29	78	208	201	73	23	174	118	109	77	176	227	154
232	42	173	97	179	8	192	161	248	61	60	107	66	49	131	79
146	254	22	25	101	224	30	202	18	134	251	19	213	215	40	102
135	178	184	167	36	105	113	48	3	114	199	164	76	217	89	236
55	156	126	159	75	142	147	58	218	219	7	38	168	45	175	234
214	186	41	5	133	221	228	63	225	1	144	235	162	50	207	163
103	81	108	88	209	165	31	127	11	80	194	187	10	198	120	153
132	98	110	148	0	100	46	250	253	57	33	32	151	14	28	150
52	12	242	252	149	106	13	95	26	96	237	177	205	243	82	85
2	239	190	140	43	203	181	6	139	238	116	64	83	44	56	245
125	70	15	51	183	27	196	39	230	121	143	35	223	128	4	21
229	244	90	111	20	62	93	145	137	67	141	185	206	233	182	59
226	249	119	160	166	200	197	240	17	117	72	37	180	171	91	74
189	222	123	122	112	169	155	193	71	212	124	24	247	129	210	170
104	255	130	152	241	65	68	99	195	136	87	53	92	231	86	34
191	84	211	188	16	138	216	172	220	69	54	246	157	115	158	94

and then encrypted. Let the output after DCT be η and the selected block be $\lambda_{M\times N}$; then, it is multiplied with an orthogonal matrix ψ and the result is stored in Φ. The values obtained in Φ are forwarded to the confusion and diffusion stage. Due to the lightweight nature of Chebyshev and intertwining maps, they are deployed in the confusion and

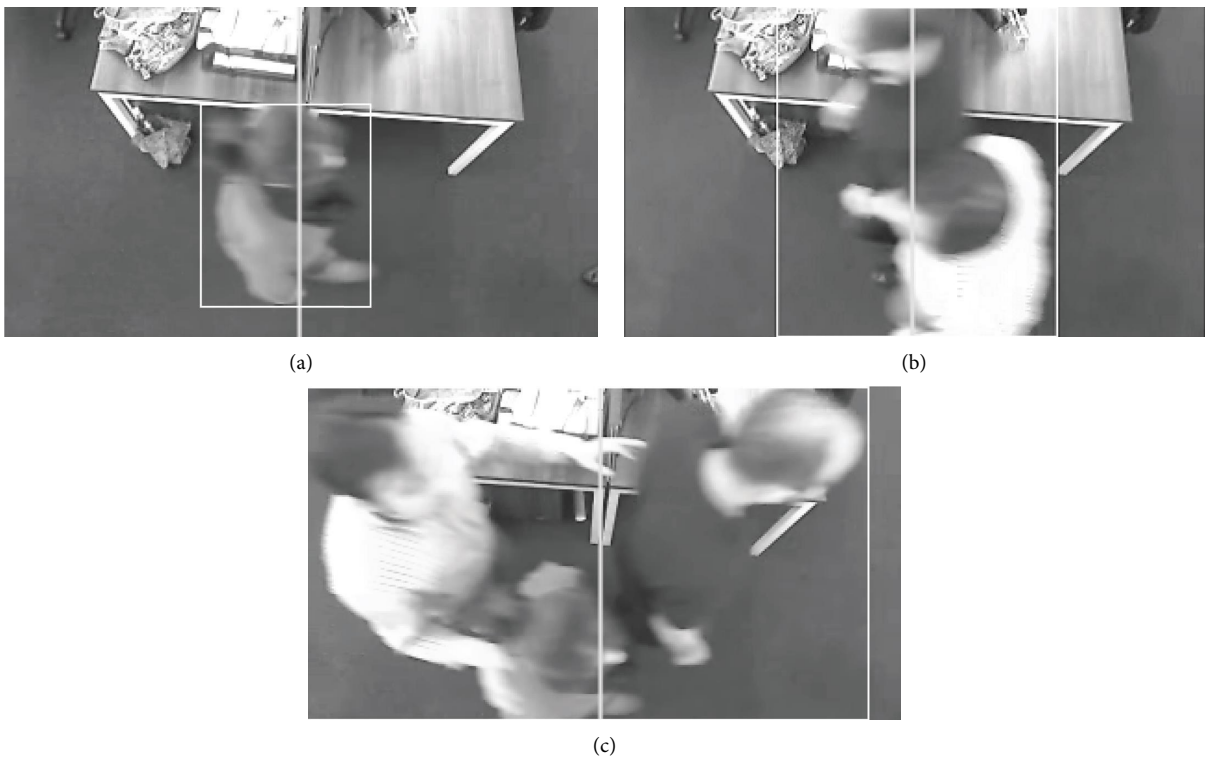


Figure 3: Real-time video frames with different number of occupants. (a) One person. (b) Two persons. (c) Three persons.

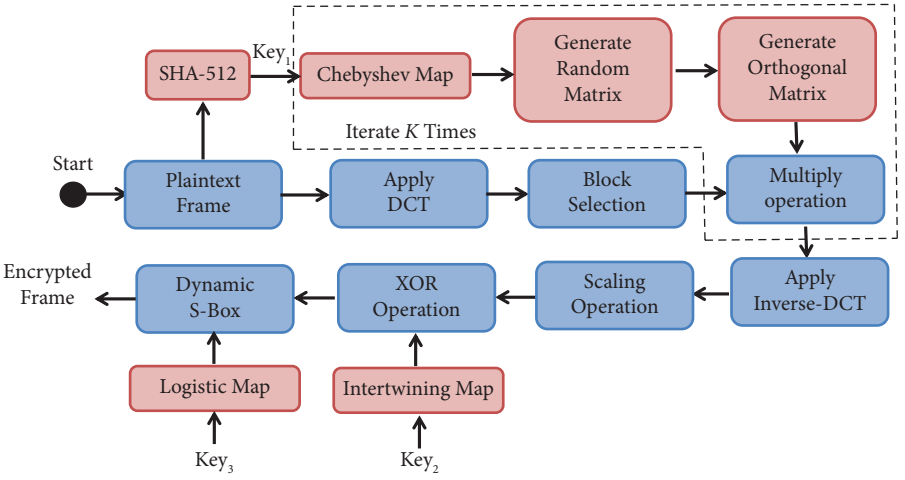


Figure 4: Flowchart of the proposed encryption-compression scheme.

diffusion process of encryption. After the encryption-compression phase, encrypted pixels are transmitted over the channel.

Let the size of a plaintext image P be $A \times B$. In this work, k represents iteration number and ranges from $k = 1$ to N, where N is the total number of iteration. When $k = 1$, the secure hash algorithm (SHA-512) is applied to the plaintext image P for the generation of initial keys for the Chebyshev map. Detailed steps of the proposed scheme are outlined as follows:

(1) Apply DCT on plaintext image P to get η.

(2) Select DCT coefficients from η, staring from the DCT-DC coefficient to get λ. The dimensions of the selected coefficients matrix can be same or different as compared to the original image. Let the size of λ be $M \times N$.

(3) Iterate a $M \times N$ Chebyshev map to get random matrix Λ.

(4) Apply the Gram–Schmidt algorithm to the random matrix Λ to get an orthogonal matrix Φ.

(5) Multiply λ and Φ and get a new matrix ϕ. Repeat steps from 3 to 5 for N times. In each iteration,

values of initial conditions are slightly changed and σ is added in original initial value, where $\sigma = 0.001$.

(6) Apply inverse DCT and map the values to the 0–255 range to get ω.

(7) Iterate a intertwining map $M \times N$ times to get a random row vector f.

(8) Multiply the row vector f with 10^{14} and apply mod operation using the following equation:

$$\alpha = \left|\left(10^{14} \times f\right)\right| \bmod (256), \tag{8}$$

where $|\cdot|$ is the absolute value. Reshape row matrix α into $M \times N$ and get β.

(9) Perform XOR operation between ω and β to get a new matrix ζ.

(10) Randomly select a S-Box using logistic map and apply S-Box on ζ to get the final ciphertext C. The output of logistic map is multiplied with a factor 10^{14} to get ψ and apply Mod 3 operator to get Ψ. If the value in Ψ is 0, 1, and 2, then AES S-Box, Khan's S-Box, and Tayseer's S-Box are selected, respectively.

Decryption is the reverse process of encryption and all steps can be applied in the reverse process to get the original plaintext image.

4. Security Analyses

Results of the proposed encryption scheme are shown in Figures 5–8. In the first test (Figure 5), the size of DCT block is the same as plaintext image size, and hence both plaintext and ciphertext image frames have same sizes. From Figure 5, one can see that the proposed scheme hides the original contents of the frame and hence the number of occupant information is also concealed. The decryption results are shown in Figure 6. In the second test, the size of DCT block is selected as $M \times N/2 \times 2$, and as a result, the size of encrypted image is 4 times less than the plaintext size. The encryption and decryption results are shown in Figures 7 and 8, respectively. In Figure 7, it can be seen that size of ciphertext is 4 times smaller than the plaintext image and still correct decryption (see Figure 8) is possible. This type of compression is not possible in traditional encryption. From the visual inspection in Figures 5 and 7, it is evident that the proposed scheme encrypts the original information; however, the security of an encryption algorithm should be statistically proved.

4.1. Correlation Coefficient. Degree of similarity between two variables can be measured via correlation coefficient metric. In image processing, correlation is the degree of similarity between two images. One can also check the correlation between two adjacent pixels (horizontal, vertical, and diagonal) through selection of random pairs. The lower the value of correlation coefficient, the higher the security of image encryption scheme.

The correlation coefficient can be computed using the following mathematical formula:

$$r = \frac{\text{Covariance}(x, y)}{S_x \times S_y}, \tag{9}$$

where S_x and S_y are standard deviation at pixel positions x and y, respectively. Covariance is written as

$$\begin{aligned} \text{cov}(x, y) &= \frac{1}{N} \sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right), \\ S_x &= \sqrt{\text{Variance}(x)}, \\ S_y &= \sqrt{\text{Variance}(y)}. \end{aligned} \tag{10}$$

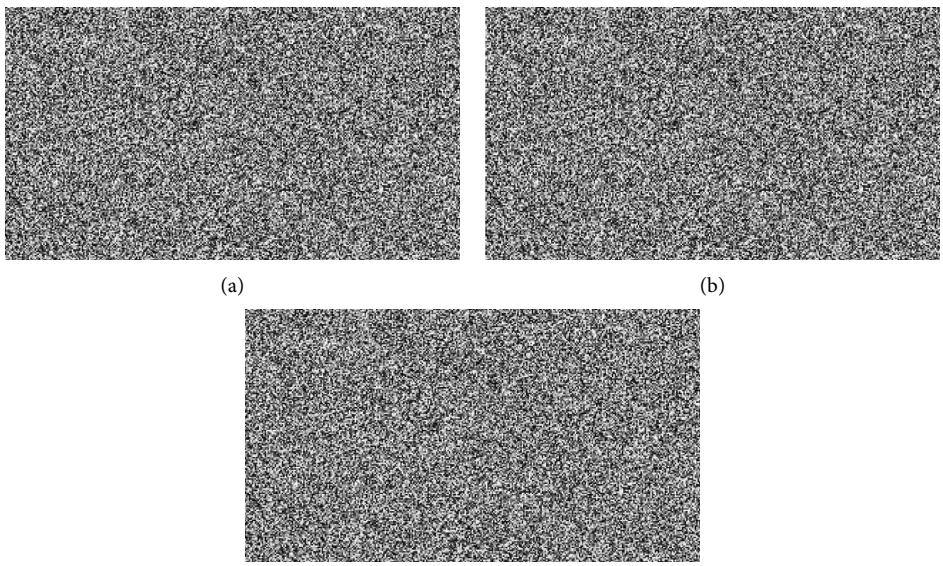
In order to check the strength of the proposed encryption scheme, we evaluated correlation coefficients in horizontal, vertical, and diagonal directions, for Figures 3 and 5, respectively. Correlation plots in diagonal direction are shown in Figure 9. From these plots, it can be seen that original images have correlated distribution in diagonal direction but encrypted images have uncorrelated distribution for all test images. Similar results were obtained for horizontal and diagonal directions. The correlation values between −1 and 1 are shown in Table 4. From the table, it is clear that when compared to the plaintext image, encrypted image has low correlation values.

4.2. Entropy. The term entropy refers to statistical measure of randomness or uncertainty. In image processing, entropy calculates the distribution of gray values. For a gray scale image with 256 gray levels, ideally the information entropy must be 8 bits for a complete random image. Mathematically, entropy is defined as

$$H(m) = \sum_{i=0}^{L-1} p(m_i) \log_2 \frac{1}{p(m_{i,})}, \tag{11}$$

where $L = 2^g$. The value of g is 8 for gray images. The entropy values of plaintext and ciphertext images are shown in Table 5. When an image is encrypted using the proposed scheme, the entropy value is close to 8.

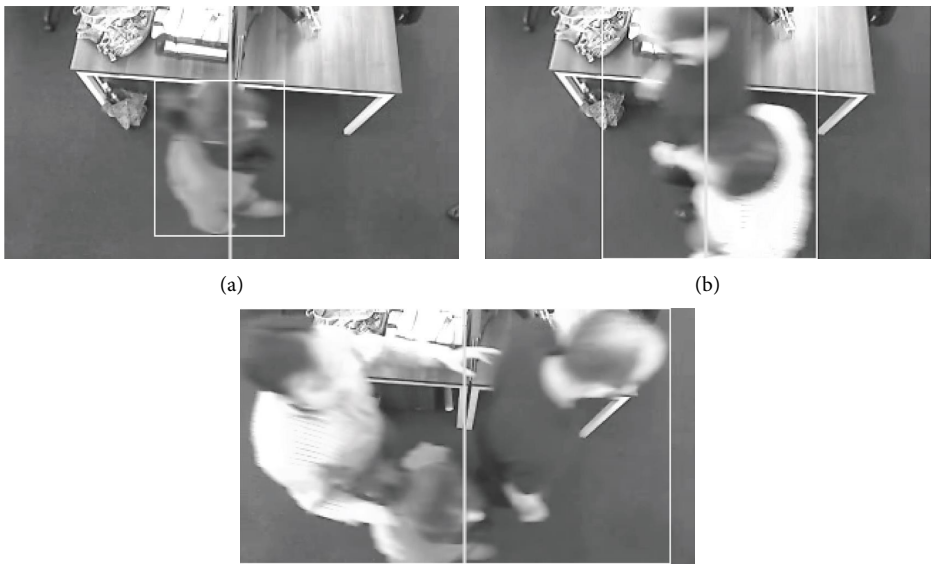
4.3. Encryption Quality. One of the important aspects in image security evaluation is to check the quality of encryption. One can check the quality of encryption via visual inspection; however, the security of encryption scheme should be mathematically proved. To check the quality of encryption, a wide range of attributes must be considered during the designing stage of an encryption scheme. Most of the attributes are outlined in our previous work [33–36]. An image encryption is considered good if it hides a wide range of those attributes. Out of many attributes, deviation in pixel values between the original and encrypted images is a robust parameter to evaluate the quality of encryption. Encryption quality is better if deviation between plaintext and ciphertext is maximum and irregular. Three different parameters can be considered to check the deviation of pixels, i.e., maximum



(a) (b)

(c)

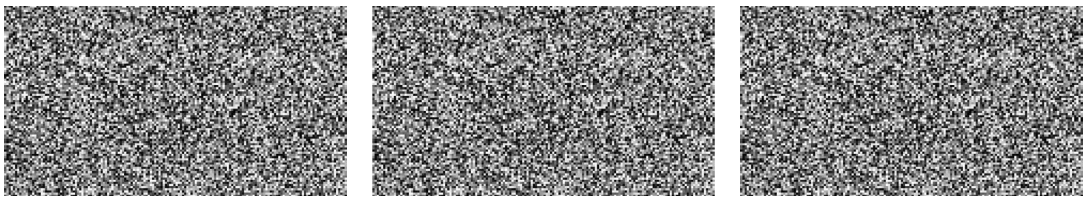
Figure 5: Real-time encryption with DCT size same as plaintext size. (a) One person. (b) Two persons. (c) Three persons.



(a) (b)

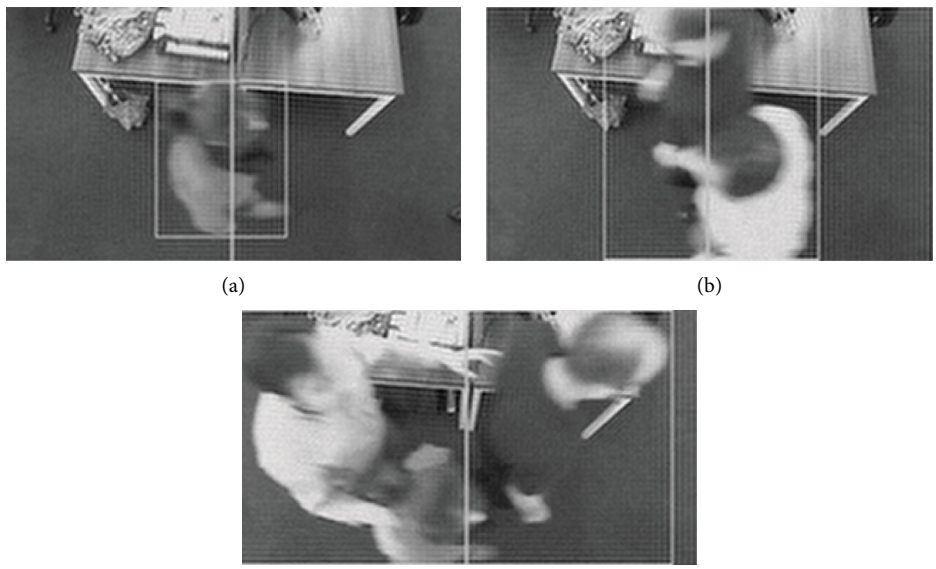
(c)

Figure 6: Decryption results of Figure 5. (a) One person. (b) Two persons. (c) Three persons.



(a) (b) (c)

Figure 7: Encryption results with DCT size $M \times N/2 \times 2$. (a) One person. (b) Two persons. (c) Three persons.



(a) (b) (c)

Figure 8: Decryption results with DCT size $M \times N/2 \times 2$. (a) One person. (b) Two persons. (c) Three persons.

deviation (MD), irregular deviation (ID), and deviation from uniform histogram (DUH).

4.3.1. Maximum Deviation (MD). MD measures the deviation between original and encrypted images. A higher value of maximum deviation indicates higher deviation. Maximum deviation is calculated in three steps:

(1) Calculate histograms for the original plaintext image P and the encrypted image C.

(2) Compute the histogram difference (HD) where HD is the absolute deviation (difference) between the histograms calculated in Step 1.

(3) Finally, compute MD as given below:

$$\mathrm{MD} = \frac{\mathrm{HD}_0 + \mathrm{HD}_{N-1}}{2} + \sum_{i=1}^{N-2} \mathrm{HD}_i, \tag{12}$$

where HD_i is the difference histogram at index i.

4.3.2. Irregular Deviation (ID). ID reveals how much of the deviation induced by the encryption algorithm on the ciphertext image is irregular. Lower value of irregular deviation indicates good encryption quality. Steps involved in the calculation of irregular deviation are given as follows:

(1) Compute the average sum of histogram values.

(2) Take the absolute difference (AD) between the average sum of histogram (Avg) and amplitude of histogram at index i (h_i). Mathematically, it is written as

$$\mathrm{AD} = \mathrm{Avg} - h_i. \tag{13}$$

(3) Finally compute ID as

$$\mathrm{ID} = \sum_{i=0}^{N-1} \mathrm{AD}. \tag{14}$$

4.3.3. Deviation from Uniform Histogram (DUH). A uniform histogram of an encrypted image is desired for good encryption quality. Less deviation from uniform histogram shows better quality of encryption. For gray scale images, ideal histogram (ID) and the deviation from uniform histogram (DUH) are measured as [37]

$$\mathrm{IH}_i = \begin{cases} \dfrac{A \times B}{256}, & 0 \le C_i \le 255, \\ 0, & \text{elsewhere.} \end{cases} \tag{15}$$

Using the above concept, Abd El-Samie et al. proposed a new metric [37] (DUH) for measuring the quality of encrypted images. DUH is calculated as [37]

$$\mathrm{DUH} = \frac{\sum_{i=0}^{255} \left| \mathrm{IH}_i - H_C \right|}{A \times B}, \tag{16}$$

where H_C is the actual histogram value of ciphertext image.

The MD, ID, and DUH are shown in Table 6. All values confirm the higher security of the proposed scheme.

4.4. Energy. Gray-level co-occurrence matrix (GLCM) is a statistical analysis of texture measurement that reflects the spatial property of image pixels. A squared sum of GLCM elements is energy. For plaintext images, some pixels have large values in gray-level co-occurrence matrix due to which the energy values are high but for ciphertext images, the values of energy are smaller because of the distributed energy values. The energy analysis can be done using the following equation.

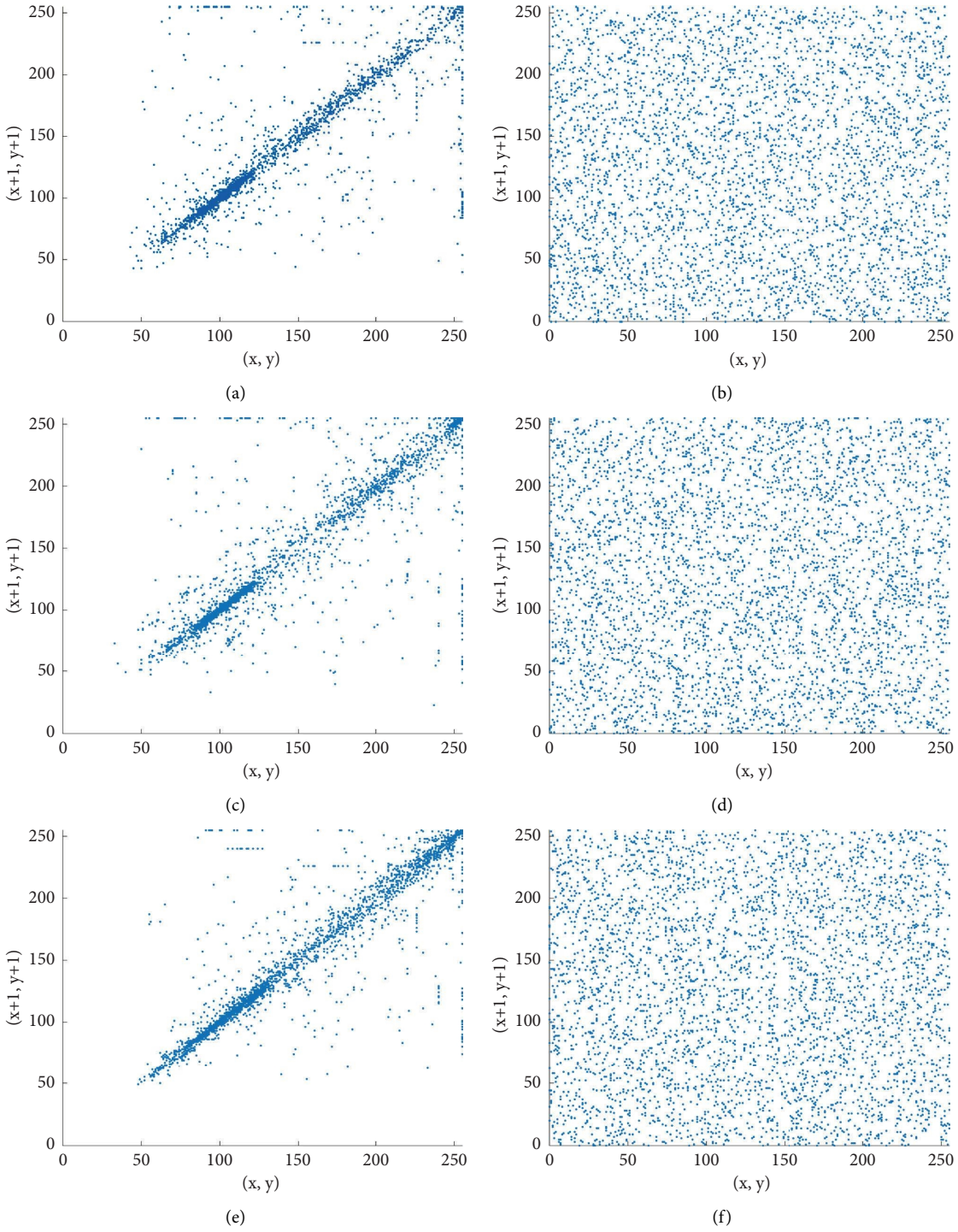


Figure 9: Plot of correlation coefficients in diagonal direction. (a) Original image (Figure 3(a) correlation plot). (b) Encrypted image (Figure 5(a) correlation plot). (c) Original image (Figure 3(b) correlation plot). (d) Encrypted image (Figure 5(b) correlation plot). (e) Original image (Figure 3(c) correlation plot). (f) Encrypted image (Figure 5(c) correlation plot).

$$E = \sum_{i,j} p(i, j)^2, \tag{17}$$

where $p(i, j)$ is the position of pixels in gray-level co-occurrence matrix. For a constant image, energy value is equal to 1. Lower values indicates higher randomness in image pixels. The energy values of the plaintext images and the corresponding ciphertext images are shown in Table 7 which shows that the energy values of the ciphertext images are very small.

4.5. Contrast. Contrast measures the variation in GLCM. With the help of contrast, a viewer can differentiate

Table 4: Correlation coefficient values for horizontal, diagonal, and vertical directions.

Images	Plaintext image			Encrypted image		
	H-D	D-D	V-D	H-D	D-D	V-D
1	0.9049	0.8347	0.9068	0.0108	−0.0134	0.0085
2	0.9081	0.8631	0.9480	0.0190	0.0253	0.0179
3	0.9580	0.9020	0.9467	0.0212	−0.0268	−0.0108

Table 5: Entropy analysis.

Images	Original image	Encrypted image
1	6.6776	7.9960
2	6.8434	7.9962
3	7.1017	7.9966

Table 6: Encryption quality analyses.

Images	MD	ID	DUH
1	5.8515×10^4	40046	0.0253
2	5.9088×10^4	37658	0.0292
3	4.8168×10^4	36622	0.0280

Table 7: Energy analysis.

Images	Original image	Ciphertext image
1	0.2631	0.0156
2	0.2487	0.0156
3	0.2159	0.0156

Table 8: Contrast analysis.

Images	Original image	Ciphertext image
1	0.4274	10.4808
2	0.6047	10.5440
3	0.3435	10.6562

Table 9: Homogeneity analysis.

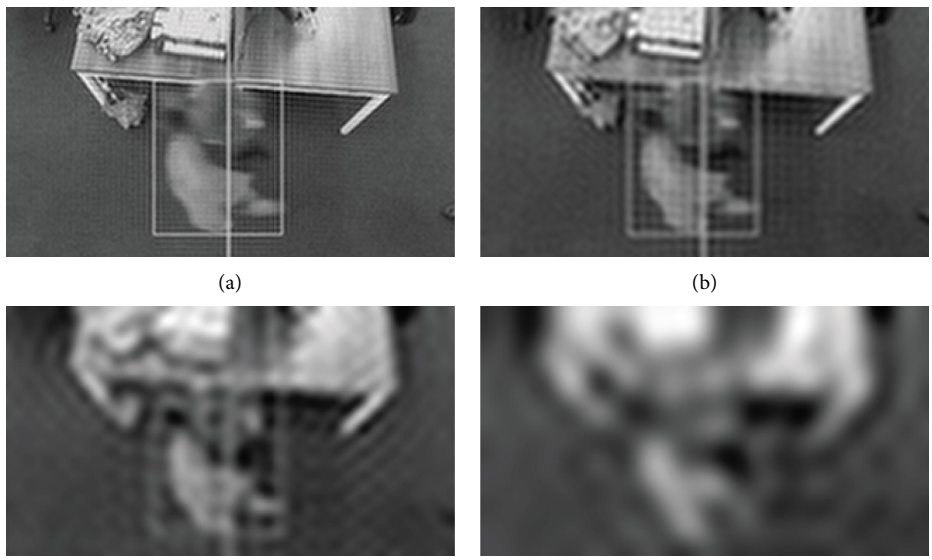
Images	Original image	Ciphertext image
1	0.9351	0.3892
2	0.9210	0.3894
3	0.9394	0.3875

Table 10: Structural content and average difference analysis.

Images	SC	AD
1	0.8228	−2.6914
2	1.0104	9.5119
3	1.1119	16.8750

Table 11: Encryption/decryption time analysis with different DCT sizes.

DCT size	Encryption time (sec)
$M\times N/2\times2$	0.0212
$M\times N/4\times4$	0.0117
$M\times N/8\times8$	0.0095
$M\times N/16\times16$	0.0092



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

Figure 10: Effect of different DCT sizes. (a) DCT size $M \times N/2 \times 2$. (b) DCT size $M \times N/4 \times 4$. (c) DCT size $M \times N/8 \times 8$. (d) DCT size $M \times N/16 \times 16$.

between the different objects of an image. A higher value of contrast is required for an encrypted image. For a constant image, the value of contrast is 0. Contrast of an image is measured as

$$C = \sum_{i,j} |i - j|^2 \times p(i, j), \tag{18}$$

where $p(i, j)$ indicates the number of GLCM. The values of contrast for plaintext images and ciphertext images are tabulated in Table 8 which clearly indicates that the contrast values of the ciphertext images are very large as compared to the contrast values of plaintext images.

4.6. Homogeneity. Another parameter that can be deduced from GLCM is homogeneity. Homogeneity is the closeness of element distribution in the GLCM. For an efficient image encryption algorithm, the homogeneity values should be low. For determination of homogeneity, the equation used is

$$\text{HOM} = \sum_{i,j} \frac{p(i, j)}{1 + |i - j|}, \tag{19}$$

where $p(i, j)$ represents the gray-level co-occurrence matrices in GLCM. The homogeneity values of the test images are shown in Table 9. It is clear from Table 9 that the proposed scheme provides higher security for plaintext images as the values of homogeneity are lower for encrypted images.

4.7. Structural Content and Average Difference. To determine the similarity between plaintext image and its corresponding ciphertext image, the structural content test can also be applied. It indicates their level of similarities. When the two images are totally different from one another, the value of structural content is 0 and a value of 1 means identical images. In case of image encryption, the value of structural content should be near 0. Mathematical expression for structural content is

$$\text{SC} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(O_{(i,j)}\right)^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(E_{(i,j)}\right)^2}, \tag{20}$$

where $O_{(i,j)}$ is the original image and $E_{(i,j)}$ is the encrypted image. Values of structural content can be observed from Table 10.

4.8. Key Space Analysis. The strength of an encryption technique is hidden in secret key parameter. Therefore, key is the most critical feature of a cryptosystem. Smaller key space may lead to expose the full key or a part of key. In digital image encryption, larger key space indicates resistance against the brute force attack. In this work, we have used three chaotic maps and total initial conditions are 8, and as a result, key space (KS) is written as

$$\begin{aligned} \text{KS} &= 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \\ &= 10^{120} \approx 2^{400}. \end{aligned} \tag{21}$$

From the above KS analysis, one can see that the proposed scheme provides sufficient larger key space and hence it is resistant to a number of exhaustive key search attacks and brute force attacks.

4.9. Computational Complexity Analysis. The proposed scheme is tested and implemented in MATLAB R2019b on a PC with 2.70 GHz CPU and 8 GB RAM. When the size of selected DCT block and plaintext image is same, encryption

Figure 11: Cameraman image.

Table 12: Security comparison.

Security parameter	Reference [39]	Reference [40]	Reference [38]	Proposed
Correlation coefficient	0.1156	−0.0012	0.4952	0.0010
Entropy	7.7015	7.9884	7.2825	7.9969
Maximum deviation	6.8×10^4	5.6×10^4	8.1×10^4	6.2×10^4
Irregular deviation	3.9×10^4	3.6×10^4	6.0×10^4	3.7×10^4
Deviation from UH	0.2629	0.0407	0.4690	0.0273
Energy	0.0174	0.0159	0.0594	0.0156
Contrast	8.9473	9.9797	1.6256	10.5064
Homogeneity	0.4587	0.3973	0.6217	0.3890

takes approximately 0.063 seconds. Decryption is the reverse process of encryption and it also takes 0.063 seconds. It is clear from Table 11 that when size of DCT block reduces, encryption time also reduces. In other traditional encryption schemes, the aforementioned feature is not available. However, one can see from Figure 10 that when size of DCT block reduces, decryption quality also reduces.

5. Comparison with Other Traditional Image Encryption Schemes

In this section, the proposed encryption scheme is compared with other state-of-the-art encryption algorithms. As cameraman (shown in Figure 11) image is most widely used in the area of image processing and image security, we have considered cameraman image in this section. The size of the cameraman image is 256×256 in this paper. Table 12 shows that the proposed technique outperforms other encryption techniques in all security metrics except MD and ID where the MD and ID are in favor of reference [38]. However, only these two metrics are not sufficient for the security. Results of all other security metrics show that the proposed technique is secure and real-time applicable.

6. Conclusion

A novel chaos-based encryption scheme is presented in this paper which can be deployed in the application of camera-based real-time secure occupancy monitoring system. The system initially transforms plaintext image to DCT coefficients and then a block from the coefficients is selected for confusion-diffusion processes. The ciphertext image size is obviously much smaller than the plaintext size, and hence the compressed ciphertext can be transmitted over a bandwidth-constrained channel. Experimental results reveal that the proposed encryption-compression system reduces overhead for channels and the ciphertext is also highly secure. Moreover, the quality of reconstructed plaintext image reduces with the size reduction of DCT coefficients. Comparison with other schemes highlighted that the proposed scheme is highly secure against a number of attacks.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Harish Kumar extends his gratitude to the Deanship of Scientific Research at King Khalid University for funding this work through research groups program under grant no. R.G.P. 2/132/42.

References

[1] K. Sun, Q. Zhao, and J. Zou, "A review of building occupancy measurement systems," *Energy and Buildings*, vol. 216, Article ID 109965, 2020.

[2] J. Ahmad, H. Larijani, R. Emmanuel, M. Mannion, and A. Javed, "Occupancy detection in non-residential buildings–a survey and novel privacy preserved occupancy monitoring solution," *Applied Computing and Informatics*, 2018.

[3] S. Aziz Shah, J. Ahmad, A. Tahir et al., "Privacy-preserving non-wearable occupancy monitoring system exploiting wi-fi imaging for next-generation body centric communication," *Micromachines*, vol. 11, no. 4, p. 379, 2020.

[4] J. Ahmad, F. Masood, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel secure occupancy monitoring scheme based on multi-chaos mapping," *Symmetry*, vol. 12, no. 3, p. 350, 2020.

[5] A. Priya, K. Sinha, M. P. Darshani, and S. K. Sahana, "A novel multimedia encryption and decryption technique using binary tree traversal, Lecture Notes in Electrical Engineering," in *Proceedings of the Second International Conference on Microelectronics, Computing & Communication Systems (MCCS 2017)*, pp. 163–178, Springer, 2019.

[6] M. Sankari and P. Ranjana, "Privacy-preserving lightweight image encryption in mobile cloud," in *Emerging Research in Computing, Information, Communication and Applications*, pp. 403–414, Springer, NY, USA, 2019.

[7] P. Rashmi, M. C. Supriya, and Q. Hua, "Enhanced lorenz-chaotic encryption method for partial medical image encryption and data hiding in big data healthcare," *Security and Communication Networks*, vol. 2022, Article ID 9363377, 9 pages, 2022.

[8] X. Xun Yi, C. H. Chik How Tan, C. K. Chee Kheong Slew, and M. Rahman Syed, "Fast encryption for multimedia," *IEEE Transactions on Consumer Electronics*, vol. 47, no. 1, pp. 101–107, 2001.

[9] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[10] A. U. Rahman, K. Sultan, D. Musleh, N. Aldhafferi, A. Alqahtani, and M. Mahmud, "Robust and fragile medical image watermarking: a joint venture of coding and chaos theories," *Journal of healthcare engineering*, vol. 2018, Article ID 8137436, 11 pages, 2018.

[11] A. Qayyum, J. Ahmad, W. Boulila et al., "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, 2020.

[12] X. Wang, L. Feng, R. Li, and F. Zhang, "A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model," *Nonlinear Dynamics*, vol. 95, no. 4, pp. 2797–2824, 2019.

[13] S. F. Raza and V. Satpute, "A novel bit permutation-based image encryption algorithm," *Nonlinear Dynamics*, vol. 95, no. 2, pp. 859–873, 2019.

[14] R. Vidhya and M. Brindha, "A chaos based image encryption algorithm using rubik's cube and prime factorization process (cierpf)," *Journal of King Saud University-Computer and Information Sciences*, 2020, In press.

[15] P. K. Naskar, S. Bhattacharyya, D. Nandy, and A. Chaudhuri, "A robust image encryption scheme using chaotic tent map and cellular automata," *Nonlinear Dynamics*, vol. 100, 2020.

[16] C.-F. Zhao and H.-P. Ren, "Image encryption based on hyper-chaotic multi-attractors," *Nonlinear Dynamics*, vol. 100, no. 1, pp. 679–698, 2020.

[17] T. S. Ali and R. Ali, "A new chaos based color image encryption algorithm using permutation substitution and boolean operation," *Multimedia Tools and Applications*, Springer, Berlin/Heidelberg, Germany, pp. 1–21, 2020.

[18] H. Liu, Y. Xu, and C. Ma, "Chaos-based image hybrid encryption algorithm using key stretching and hash feedback," *Optik*, vol. 216, Article ID 164925, 2020.

[19] X. Chai, X. Fu, Z. Gan, Y. Zhang, Y. Lu, and Y. Chen, "An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata," *Neural Computing & Applications*, vol. 32, no. 9, pp. 4961–4988, 2020.

[20] F. Musanna, D. Dangwal, S. Kumar, and V. Malik, "A chaos-based image encryption algorithm based on multiresolution singular value decomposition and a symmetric attractor," *The Imaging Science Journal*, vol. 68, no. 1, pp. 24–40, 2020.

[21] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional fourier transform and dna sequence operation," *Optics & Laser Technology*, vol. 121, p. 105777, 2020.

[22] J. Karmakar and M. K. Mandal, "Chaos-based image encryption using integer wavelet transform," in *Proceedings of the 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 756–760, IEEE, Noida, India, February 2020.

[23] X.-H. Song, H.-Q. Wang, S. E. Venegas-Andraca, and A. A. Abd El-Latif, "Quantum video encryption based on qubit-planes controlled-xor operations and improved logistic map," *Physica A: Statistical Mechanics and Its Applications*, vol. 537, Article ID 122660, 2020.

[24] D. Abbasinezhad-Mood, A. Ostad-Sharif, S. M. Mazinani, and M. Nikooghadam, "Provably-secure escrow-less Chebyshev chaotic map-based key agreement protocol for vehicle to grid connections with privacy protection," *IEEE Transactions on Industrial Informatics*, vol. 16, 2020.

[25] X. Li, J. Niu, S. Kumari et al., "A novel chaotic maps-based user authentication and key agreement protocol for multi-server environments with provable security," *Wireless Personal Communications*, vol. 89, no. 2, pp. 569–597, 2016.

[26] X. Kang, Y. Chen, F. Zhao, and G. Lin, "Multi-dimensional particle swarm optimization for robust blind image watermarking using intertwining logistic map and hybrid domain," *Soft Computing*, vol. 24, no. 14, Article ID 10561, 2020.

[27] J. S. Khan, S. K. Kayhan, S. S. Ahmed et al., "Dynamic s-box and pwlcm-based robust watermarking scheme," *Wireless Personal Communications*, vol. 125, pp. 1–18, 2022.

[28] N. A. Azam, U. Hayat, and M. Ayub, "A substitution box generator, its analysis, and applications in image encryption," *Signal Processing*, vol. 187, Article ID 108144, 2021.

[29] J. Daemen and V. Rijmen, *The Design of Rijndael: The Advanced Encryption Standard (AES)*, Springer Nature, NY, USA, 2020.

[30] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel substitution box for encryption based on lorenz equations," in *Proceedings of the 2017 International Conference on Circuits, System and Simulation (ICCSS)*, pp. 32–36, IEEE, London, UK, July 2017.

[31] T. K. Alshekly, E. A. Albahrani, and S. H. Lafta, "4d chaotic system as random substitution-box," *Multimedia Tools and Applications*, vol. 81, pp. 1–22, 2022.

[32] W.-H. Wen-Hsiung Chen, C. Smith, and S. Fralick, "A fast computational algorithm for the discrete cosine transform," *IEEE Transactions on Communications*, vol. 25, no. 9, pp. 1004–1009, 1977.

[33] J. Ahmad, S. O. Hwang, and A. Ali, "An experimental comparison of chaotic and non-chaotic image encryption schemes," *Wireless Personal Communications*, vol. 84, no. 2, pp. 901–918, 2015.

[34] J. Ahmad and S. O. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," *Nonlinear Dynamics*, vol. 82, no. 4, pp. 1839–1850, 2015.

[35] J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimedia Tools and Applications*, vol. 75, no. 21, Article ID 13951, 2016.

[36] J. Arif, M. A. Khan, B. Ghaleb et al., "A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution," *IEEE Access*, vol. 10, Article ID 12966, 2022.

[37] F. E. Abd El-Samie, H. E. H. Ahmed, I. F. Elashry et al., *Image Encryption: A Communication Perspective*, CRC Press, Boca Raton, Florida, 2013.

[38] K. A. K. Patro, M. Prasanth Jagapathi Babu, K. Pavan Kumar, and B. Acharya, "Dual-layer DNA-encoding-decoding operation based image encryption using one-dimensional chaotic map," *Advances in Data and Information Sciences*, vol. 94, pp. 67–80, 2020.

[39] A. Anees, A. M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly autocorrelated data in encryption algorithm," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 9, pp. 3106–3118, 2014.

[40] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Systems and Signal Processing*, vol. 30, no. 2, pp. 943–961, 2019.