Efficient Segment-based Image Ciphering using Discretized Chaotic Standard Map with ECB, OFB and CBC

Mohammed A. AlZain
Department of Information Technology, College of Computers and Information Technology
Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia

***Abstract*—This paper presents a block-based ciphering scheme that employs the 2D discretized chaotic Standard map (CSM) in three different operation modes. The employed operation modes include the electronic codebook (ECB), the output feedback (OFB) and the cipher block chaining (CBC) modes. In the presented 2D discretized CSM with the OFB and CBC, the initiation vector (IV) is employed as the primary secret key. The presented 2D discretized CSM with the CBC has two merits. The first merit is the ability of the presented 2D discretized CSM with the ECB, OFB and CBC to encipher images of any dimensions in a comparatively short time. The second merit is the high level of security of the presented 2D discretized CSM with the OFB and CBC through the integration of both diffusion and confusion operations. Different security key metrics like histogram deviation, irregular, and coefficient of correlation, are examined to assess the functionality of the presented 2D discretized CSM with the OFB and CBC. The resistance to noise, uniformity of histogram, and encryption speed are also investigated. The suggested 2D discretized CSM with the OFB and CBC is compared with the 2D discretized CSM in ECB. The achieved outcomes demonstrate that the proposed 2D discretized CSM with the OFB and CBC has a high security than in ECB from cryptographic viewpoint. Also, achieved outcomes demonstrate that the proposed 2D discretized CSM has better noise immunity in OFB compared with ECB and OFB.**

Keywords*—*Cryptography; 2D discretized CSM; ECB; OFB; CBC

I. Introduction

The cryptography field is especially important in the modern era, where information security is paramount. Security is an important issue for image communications and storage, and ciphering is considered as one of the most important ways to realize and ensure security. Ciphering has a lot of applications such as online communications, multimedia communications, medical image protection, telemedicine, military communications, pay TV, and video conferencing. Chaotic ciphering has an important role in current cryptography. The attraction of utilizing chaotic ciphering for implementing the current cryptosystems is due to several reasons which satisfy the traditional Shannon requirements of both diffusion and confusion [1-3]. These reasons may include its random-like behavior and parameters setting sensitivity and preconceived conditions [4]. Chaotic-based schemes have demonstrated some positive features in many of the affected areas in terms of speed, integration complexity, security, power, and computational overhead. Now, some ciphers for securing images have been presented [5-8]. Other cryptosystems based on discrete chaotic systems have been suggested, but still they have some concerns about their security [9-15].

Actually, there exists two basic ways to approach digital images chaotic ciphering. In the first approach, a chaos-based stream cipher model is employed for generating pseudo-random access keys to hide the source plaintext [16]. This model is known as stream cipher. In the other scheme, the source text or secret key can be employed as initialization conditions or control parameters, and the chaotic system is iterated for several rounds to deliver the final encrypted data [17-18]. This model is known as block cipher. Now, the chaotic 2D maps have been developed into 3D to design symmetric cryptosystems, which are intended to increase security. The 3D chaotic Baker mapping introduced by Mao et al. and 3D chaotic Cat mapping introduced by Chen et al. [19-20] represent some examples of 3D chaotic maps.

In the article, a block-based ciphering scheme that employs the 2D discretized CSM with the ECB, OFB and CBC is presented. In the presented 2D discretized CSM with the OFB and CBC, the image is split into blocks, and the encryption is applied for each one of these blocks using the 2D discretized CSM with the ECB, CBC and OFB. The initiation vector (IV) is employed as the primary secret key. The 2D discretized CSM with the CBC provides two advantages. The first is the ability of the presented 2D discretized CSM with the ECB, OFB and CBC to encipher images of any dimensions in a comparatively short time. The second one is the high level of security of the presented 2D discretized CSM with the ECB, OFB and CBC through the integration of both diffusion and confusion operations. Several security key performance metrics like histogram deviation, irregular, and coefficient of correlation, are examined to assess the functionality of the presented 2D discretized CSM with the ECB, OFB and CBC. The resistance to noise, uniformity of histogram, and encryption speed are also investigated. The suggested 2D discretized CSM with the ECB, OFB and CBC is compared with the 2D discretized CSM and the RC5. The achieved outcomes demonstrate that the proposed 2D discretized CSM with the ECB, OFB and CBC has a high security from cryptographic viewpoint.

The remainder of this paper is structured as follows. Section II provides an overview of the traditional 2D CSM, 2D discretized CSM in addition to the utilized ECB, OFB and CBC operation modes. Section III presents the introduced image cryptosystem using 2D discretized CSM with the ECB, OFB and CBC. Section IV gives the design issues of the proposed image cryptosystem using 2D discretized CSM with the ECB, OFB and CBC cryptosystem. Section V provides encryption quality metrics used to evaluate the performance of the proposed image cryptosystem using 2D discretized CSM with the ECB, OFB and CBC. Section VI provides the results of the presented image cryptosystem using 2D discretized CSM with the ECB, OFB and CBC. Finally, the paper conclusions are listed in Section VII.

II. Preliminary Tools

This part provides a compact overview for three conventional cryptosystems, the 2D CSM, 2D discretized CSM, and RC5 ciphers in addition to the utilized ECB, OFB and CBC operation modes. All of 2D CSM, 2D with the ECB, OFB and CBC are symmetric block ciphers. In both crypto ciphers, the utilized key is the same for both of encryption and decryption.

A. The 2D Chaotic Standard Map (2D CSM) and 2D Discretized CSM Cipher

With chaos-based image ciphering, the positions of pixels are arbitrarily changed. Different chaotic-based maps may be employed with chaos-based image ciphering like 2D Cat, 2D Henon, 2D Baker, line, and General maps. The Standard mapping, Cat mapping, Henon mapping, and Baker mapping employ processes of geometric modifications. The line mapping employs stretching of the whole pixels form a straight line, and employs folding according to certain rules. Then, the plainimage pixels are chaotically distributed in the resulted cipherimage and nearby pixels are no longer important. On contrary, a typical 2D CSM was developed by Boris Chirikov in 1969. The 2D CSM with continuous confusion is described as follows [21]:

$$\begin{bmatrix} u(i+1) \\ v(i+1) \end{bmatrix} = \begin{bmatrix} \big(u(i)+v(i)\big) \bmod 2\pi \\ \big(v(i)+k\sin u(i+1)\big) \bmod 2\pi \end{bmatrix} \tag{1}$$

If Eq. 1 is discretized, it will be mapped from [0,2π], to M×M through putting $u = u\text{M}/2\pi$, $v=v\text{M}/2\pi$, and $\text{k}=\text{kM}/2\pi$ to transform the 2D CSM to the 2D discretized CSM as follows [21]:

$$\begin{bmatrix} u(i+1) \\ v(i+1) \end{bmatrix} = \begin{bmatrix} \big(u(i)+v(i)\big) \bmod M \\ \left(v(i)+K\sin\dfrac{u(i+1)M}{2\pi}\right) \bmod M \end{bmatrix} \tag{2}$$

where k denotes a non-negative integer.

If the 2D discretized CSM is employed for image ciphering, u(i) and v(i) represent the pixel coordinates of the plainimage. u(i + 1) and v(i + 1) represent the pixel coordinates of the cipherimage.

The 2D discretized CSM is intended to achieve continuous map properties; it must be very close to the base map as the number of pixels is usually endless [21]. The resulted cipher of the 2D discretized CSM is a permutation cipher, which cannot modify the cipherimage histogram from its corresponding plainimage. Since this cipher is simple and fast, it does provide a high level of security, and its processing time grows as image dimensions increases.

B. The ECB Mode

The ECB mode starts through segmenting the input data into segments of equal sizes as illustrated in Fig. 1(a). Then every segment is separately encrypted using the same encryption key. The ECB operation mode can be mathematically represented using the following equation:

$$\text{Cipher}_{\text{j}}= \text{ENC}_{\text{k}}\ (\text{Plain}_{\text{j}}),\ \ \text{j}=1,2,3,\ldots..,\text{n} \tag{3}$$

The ECB deciphering process can be represented as:

$$\text{Plain}_{\text{j}}= \text{DEC}_{\text{k}}(\text{Cipher}_{\text{j}}),\ \ \text{j}=1,2,3,\ldots..,\text{n} \tag{4}$$

C. The OFB Mode

The OFB mode starts through ciphering the IV as illustrated in Fig. 1(b). Then, the resulted output bits are XORed with their corresponding plaintext block to result in the ciphertext block. In addition, the resulted ciphertext block bits are utilized an input IV to the next stage. The procedure is repeated till reaching the final block. The OFB operation mode can be mathematically represented using the following equation:

$$\text{Cipher}_{\text{j}}= \text{Plain}_{\text{j}} \oplus \text{I}_{\text{j}}\ ,\ \ \text{j}=1,2,3,\ldots..,\text{n} \tag{5}$$

The OFB deciphering process can be represented as:

$$\text{Plain}_{\text{j}}= \text{Cipher}_{\text{j}} \oplus \text{I}_{\text{j}}\ \ \ \text{j}=1,2,3,\ldots..,\text{n} \tag{6}$$

where $\text{I}_{\text{j}}= \text{ENC}_{\text{k}}\ (\text{I}_{\text{j-1}})$, j=1, 2, 3…n, and $\text{I}_0 = \text{IV}$.

As CBC mode, ciphering phase should be strong enough to provide efficient immunity to any attack attempts to break it.

D. The CBC Operation Mode

The CBC operation mode is a segment encryption mechanism as illustrated in Fig. 1(c). The CBC operation mode has been employed for use with the 2D discretized CSM in the introduced cipher. In the introduced 2D discretized CSM cipher with CBC, the CBC mode utilizes IV of equivalent size to the segmented block size. First, each one of IV pixels is XORed with its corresponding block pixel in the 1st block. After that, the outgoing pixels are ciphered. The first block pixels are employed as IV to encipher the second block. The process is repeated with the same sequence until reaching the final block. The CBC operation mode can be mathematically represented using the following equation:

$$\text{Cipher}_{\text{j}}=\text{ENC}_{\text{k}}\ (\text{Cipher}_{\text{j-1}}\oplus \text{Plain}_{\text{j}}),\ \text{j}=1,\ 2,\ 3,\ldots..,\ \text{n} \tag{7}$$

where Cipher_0 =IV, Cipher_{j} denotes the ciphered block, ⊕ represents the XOR operation, and ENK_{k} denotes the 2D CSM encryption.

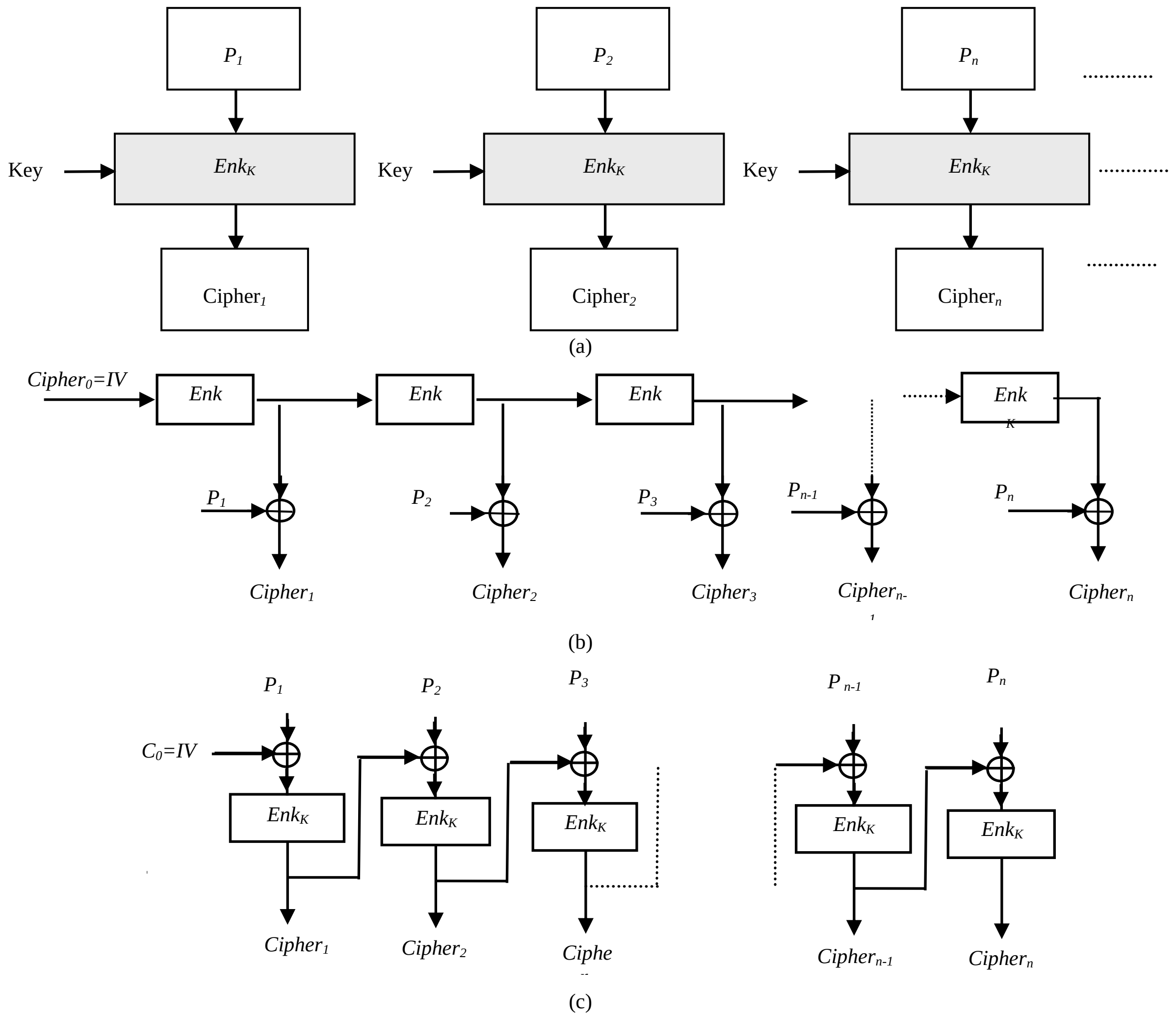

Fig. 1. The Employed ECB, OFB and CBC with Introduced 2D Discretized CSM Cipher as Depicted in (a), (b) and (c).

The CBC operation mode employs an integration method that employs dependence on each cipherimage block for all the previous cipherimage blocks. As a consequence, all eligibility for all previous cipherimage blocks is contained in the previous cipherimage blocks [22]. The CBC basic drawback disadvantage lies in the fact that an attack on just single cipherimage segment affects two plainimage segments when employing decryption [23]. The CBC deciphering process can be represented as:

$$\text{Plain}_j = \text{DEC}_k\,(\text{Cipher}_j)\oplus\text{Cipher}_{j-1},\ \ j=1, 2, 3,\ldots,n \qquad (8)$$

where DEC_k denotes the deciphering procedure.

III. Proposed 2D discretized CSM-based Image Cipher with OFB and CBC Operation Modes

This part is to provide an overview of the introduced 2D discretized CSM cipher with the ECB, OFB and CBC. The proposed 2D discretized CSM cipher with the ECB, OFB and CBC is designed with the potential of enhancing the security the cipherimage and providing a reasonable encryption/decryption speeds. For realizing these objectives, 2D discretized CSM encryption is employed with the ECB, OFB and CBC [24-29]. Three schemes of the 2D discretized CSM with ECB, OFB and CBC are examined to determine which operation mode that will increase the efficiency of the proposed 2D discretized CSM cipher.

The operation of the proposed 2D discretized CSM cipher with the ECB, OFB and CBC may be summed up as shown below in the next three steps. The steps of the proposed 2D discretized CSM cipher with the ECB, OFB and CBC is depicted can be listed as:

1) The plainimage to be encrypted is scanned line by line.

2) The scanned image is segmented into blocks of; each block of has n x n pixels.

3) The segmented image blocks are ciphered using the proposed 2D discretized CSM cipher with the ECB, OFB and CBC modes of operation as depicted in Fig. 1.

IV. Design Points of the 2D discretized CSM cipher with the OFB and CBC

As mentioned previously, the proposed 2D discretized CSM cipher may be employed in ECB, OFB and CBC operating modes. It basically employs a 2D discretized CSM with the ECB, OFB and CBC as the main cipher scheme. It is well known that scrambling employed in the 2D discretized CSM resembles like random behaviour [30]. The proposed 2D discretized CSM cipher with the OFB and CBC employs IV as a primary key. The IV should be random to be resistant against various types of brute force attacks. The utilized XOR among the IV fragments and data block fragments modifies pixel values, making the proposed 2D discretized CSM cipher with the ECB, OFB and CBC like a standard 3-D map. The proposed 2D discretized CSM cipher with the ECB, OFB and CBC also employs a secondary key, which is utilized in the 2D discretized CSM to shuffle pixels.

Finally, the proposed 2D discretized CSM cipher with the ECB, OFB and CBC image cryptosystem depends on segmenting the images to be cipher into various segments. The segment size in bits considered of a significant factor for affecting the performance of the proposed 2D discretized CSM cipher with the ECB, OFB and CBC. The segment size impact on cipher quality is examined in details in the experimental results part. Since the Section IV provides an equivalent bits size as plaintext segment size, increasing the segment size will result in increasing the security. In addition, the proposed 2D discretized CSM cipher with the ECB, OFB and CBC has the ability for encrypting digital images of any size after splitting them into smaller segments.

V. Cipher Quality Key Indicators

The cipher quality testing is very important for image cipher. Visual encryption quality is not sufficient for this test. So, there is a need for mathematical cipher quality key indicator metrics. Here, four cipher quality indicators will be considered to assess and compare the effectiveness of the proposed 2D discretized CSM cipher with the ECB, OFB and CBC. These quality key indicator metrics include correlation coefficient, irregular deviation, and deviations of histogram. In addition, two other quality key indicator metrics are also considered to assess cipher quality; histogram uniformity, and computational time [31-40].

A. The Correlation Coefficient

The correlation coefficient may be considered as a significant estimation for assessing the ciphering quality of any image cipher. As the correlation coefficient becomes near zero, the performance of the image cipher becomes good [31-32]. The correlation coefficient can be estimated as follows [31-32]:

$$CC = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{9}$$

where *x* and *y* denotes the pixels intensity levels at the same location in both the plainimage and ciphered image. The definitions for the covariance, standard deviation and mean are given below as follows:

$$\operatorname{cov}(x,y) = \frac{1}{L}\sum_{i=l}^{L}(x(i) - E(x))(y(i) - E(y)) \tag{10}$$

$$D(x) = \frac{1}{L}\sum_{i=l}^{L}(x(i) - E(x))^2 \tag{11}$$

$$D(y) = \frac{1}{L}\sum_{i=l}^{L}(y(i) - E(y))^2 \tag{12}$$

where, L denotes the pixels number. As the correlation becomes near zero, the better the image cipher quality.

B. Histogram Distribution

The cipherimage histogram distribution can be utilized as an indicator for assessing the quality of the proposed 2D CSM cipher with the ECB, OFB and CBC. As the cipherimage has a uniform histogram distribution, the proposed 2D CSM cipher with the ECB, OFB and CBC has a good ciphering quality.

C. The Irregular Deviation

The irregular may be employed for assessing the ciphering quality in terms of how much it can reduce the deviation to be near the histogram of an ideally ciphered image [33-35]. The process of estimating the irregular deviation starts by calculating the absolute deviation among the plainimage and the enciphered image. After that it calculates the histogram of the resulted absolute deviation. Then, calculate the mean histogram of the resulted absolute deviation. Finally, calculate the histogram deviation absolute mean value.

The irregular deviation can be computed as given below:

$$D_I = \frac{\left|\sum_{i=0}^{255}\left|H(i) - M_H\right|\right|}{MxN} \tag{13}$$

As the irregular deviation becomes low, the performance of the image cipher becomes good.

D. The Deviation of Histogram

The deviation of histogram can be employed for assessing the ciphering quality in terms of how much it can magnify the difference among the plainimage and the enciphered image [36-38]. The process of estimating the deviation of histogram starts by calculating the histogram of the plainimage and the enciphered image. After that, calculate the absolute deviation among histogram of the plainimage and the enciphered image. Finally, compute the curve area beyond the absolute deviation divided by the total image area as follows [36-38]:

$$D_H = \frac{\left(\frac{d_0 + d_{255}}{2} + \sum_{i=1}^{254} d_i\right)}{MxN} \tag{14}$$

where d_i denotes is the absolute difference curve magnitude at intensity level *i*, *M* and *N* denote the image dimensions. As the deviation of histogram becomes high, the performance of the image cipher becomes good [25].

E. The Impact of Noise

Noise immunity demonstrates the cipher capability to withstand and against the noise. To examine and measure the impact of noise on the proposed 2D discretized CSM cipher with the ECB, OFB and CBC, noises of various SNRs are added to cipherimages, and after that the deciphering procedure is applied. If the resulted deciphered image is very close to its corresponding plainimage, it could mean that the proposed 2D discretized CSM cipher with the ECB, OFB and CBC has a capability to resist the noise [39-42]. This proximity can be ensured numerically or visually using the correlation coefficients and the PSNR of the deciphered image, which can be denoted as follows [39-42]:

$$PSNR = 10 \times \log_{10}\left(\frac{M \times N \times 255^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}\left|\left(f(m,n) - f_d(m,n)\right)\right|^2}\right) \tag{15}$$

where $f(m,n)$ denotes the plainimage and $f_d(m,n)$ denotes its corresponding deciphered image.

VI. Experimental Tests and Discussion

In experimental tests, test experiments were employed to investigate and examine the proposed 2D discretized CSM cipher with the ECB, OFB and CBC With respect to the proposed 2D discretized CSM cipher with the ECB, OFB and CBC, the IV is employed as a portion of the enciphered Pirate image, and has an equivalent size with respect to the chosen segment size. Various segments of different sizes were examined in testing the proposed 2D discretized CSM cipher with the ECB, OFB and CBC as shown below:

1) S_1 = IV = 4 × 4 with IV as a portion of the enciphered Pirate image.

2) S_2 = IV = 8 × 8 with IV as a portion of the enciphered Pirate image.

3) S_3 = IV = 16 × 16 with IV as a portion of the enciphered Pirate image.

4) S_4 = IV = 32 × 32 with IV as a portion of the enciphered Pirate image.

5) S_5 = IV = 64 × 64 with IV as a portion of the enciphered Pirate image.

6) S_6 = IV = 128 × 128 with IV as a portion of the enciphered Pirate image.

7) S_7 = IV = 256 × 256 with IV as a portion of the enciphered Pirate image.

The enciphered Pirate images using the proposed 2D discretized CSM cipher with the ECB, OFB and CBC and various segment sizes are depicted in Fig. 2. It is clearly noted from Fig. 2 that the proposed 2D discretized CSM cipher with the OFB and CBC has a better performance than the proposed 2D discretized CSM cipher with ECB especially with small segment sizes. Also, with increasing the segment size, the proposed 2D discretized CSM cipher with the OFB and CBC has a good performance in hiding all the details of the enciphered images.

The histograms distribution of Pirate plainimage and its enciphered image using the 2D discretized CSM image cipher with the ECB, OFB and CBC are depicted in Fig. 3. It is clearly noted from Fig. 3 that the 2D discretized CSM image cipher with ECB does not provide histogram uniformity and it has the same histogram of the original Pirate plainimage. This is due to the fact that the 2D discretized CSM image cipher with ECB performs just permutation which does not change the histograms of the encrypted images which may be considered as a basic weakness. Finally, it is clear from Fig. 3 that the 2D discretized CSM image cipher with the OFB and CBC can provide histogram uniformity.

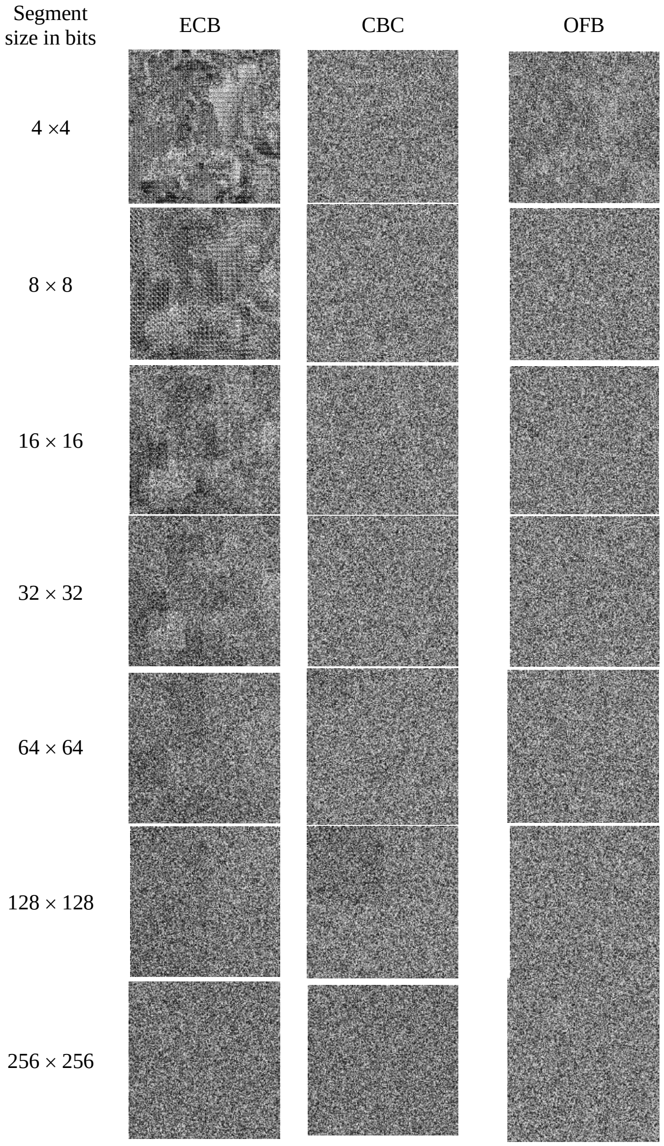

Fig. 2. Enciphered Pirate Images using the Proposed 2D Discretized CSM Cipher with the OFB and CBC with Various Segment Sizes.

Tables I, II, and III illustrates the numerical estimations of the evaluated key performance metrics like correlation coefficient (CC), irregular deviation (ID) and maximum deviation (MD) for the proposed 2D discretized CSM cipher with the ECB, OFB and CBC and various segment sizes.

The CC outcomes results listed in Table I demonstrated that the proposed 2D discretized CSM cipher with the OFB and CBC has lower CC values than in the proposed 2D discretized CSM cipher with the ECB. Also, with increasing the segment size, the CC values of the proposed 2D discretized CSM cipher with the ECB, OFB and CBC becomes near the zero value.

The ID outcomes results listed in Table II demonstrated that the proposed 2D discretized CSM cipher with the OFB and CBC has lower ID values than in the proposed 2D discretized

CSM cipher with the ECB. Also, with increasing the segment size, the ID values of the proposed 2D discretized CSM cipher with the ECB, OFB and CBC decrease.

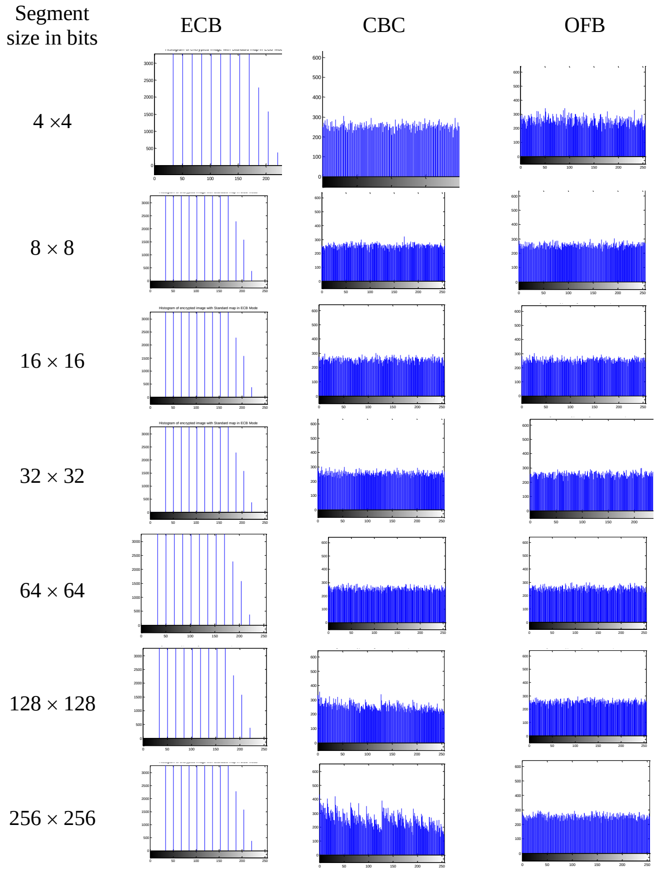

Fig. 3. Histogram of Enciphered Pirate Images using the Proposed 2D Discretized CSM Cipher with the OFB and CBC with Various Segment Sizes.

The MD outcomes results are listed in Table III and the outcomes results demonstrated that the 2D discretized CSM image cipher with ECB provides zero MD values. This is due to the fact that the 2D discretized CSM image cipher with ECB performs just permutation which does not change the histograms of the encrypted images.

Also, the proposed 2D discretized CSM cipher with the OFB and CBC has better MD values than in the proposed 2D discretized CSM cipher with the ECB.

TABLE I. CC OF ENCIPHERED PIRATE IMAGES USING THE PROPOSED 2D DISCRETIZED CSM CIPHER WITH THE ECB, OFB AND CBC WITH VARIOUS SEGMENT SIZES

Segment size in bits	ECB	CBC	OFB
4 ×4	0.1715	-0.0043	0.1156
8 × 8	0.1307	-0.0075	-0.0159
16 × 16	0.1326	-0.00092	-0.0198
32 × 32	0.0765	0.0028	-0.0105
64 × 64	0.0497	-0.0054	0.0044
128 × 128	0.0351	0.0233	0.0028
256 × 256	0.0086	0.0066	-0.0086

TABLE II. ID OF ENCIPHERED PIRATE IMAGES USING THE PROPOSED 2D DISCRETIZED CSM CIPHER WITH THE OFB AND CBC WITH VARIOUS SEGMENT SIZES

Segment size in bits	ECB	CBC	OFB
4 ×4	0.7891	0.6667	0.7489
8 × 8	0.7300	0.6655	0.6677
16 × 16	0.7400	0.6676	0.6647
32 × 32	0.7130	0.6715	0.6655
64 × 64	0.7038	0.6679	0.6690
128 × 128	0.6984	0.6844	0.6711
256 × 256	0.6840	0.6837	0.6682

TABLE III. MD OF ENCIPHERED PIRATE IMAGES USING THE PROPOSED 2D DISCRETIZED CSM CIPHER WITH THE OFB AND CBC WITH VARIOUS SEGMENT SIZES

Segment size in bits	ECB	CBC	OFB
4 ×4	0	1.8963	1.8920
8 × 8	0	1.8978	1.9002
16 × 16	0	1.8988	1.8988
32 × 32	0	1.8980	1.8986
64 × 64	0	1.8934	1.8970
32 × 128	0	1.9020	1.8977
256 × 256	0	1.8992	1.8969

To examine the impact of the noise for the proposed 2D discretized CSM cipher with the ECB, OFB and CBC, the additive white Gaussian noise (AWGN) of SNR equals to 5 dB is summed to the enciphered Pirate image, and the deciphering procedure is applied. The deciphering outcome results of the proposed 2D discretized CSM cipher with the ECB, OFB and CBC and various segment sizes are depicted in Fig. 4. It is clearly noted from Fig. 4 that the proposed 2D discretized CSM cipher with the OFB has a better performance than the proposed 2D discretized CSM cipher with the ECB and CBC with small segment sizes. Also, the proposed 2D discretized CSM cipher with the OFB is more resistant to noise than the proposed 2D discretized CSM cipher with the ECB and CBC.

In addition, the OFB and CBC operation modes provide approximately equivalent performance in the existence of noise. Finally, the segment size has no impact on noise resistance of the proposed 2D discretized CSM cipher with the ECB, OFB and CBC.

Table IV and Table V illustrate the numerical estimations of the evaluated key performance metrics like PSNR and CC for the proposed 2D discretized CSM cipher with the ECB, OFB and CBC and various segment sizes. These PSNR and CC numerical key performance indicator values are estimated in the AWGN existence of SNR equals 5 dB. The PSNR and CC results listed in Table IV and Table V demonstrated that the proposed 2D discretized CSM cipher with the OFB has a better PSNR and CC than the proposed 2D discretized CSM cipher with the ECB and CBC.

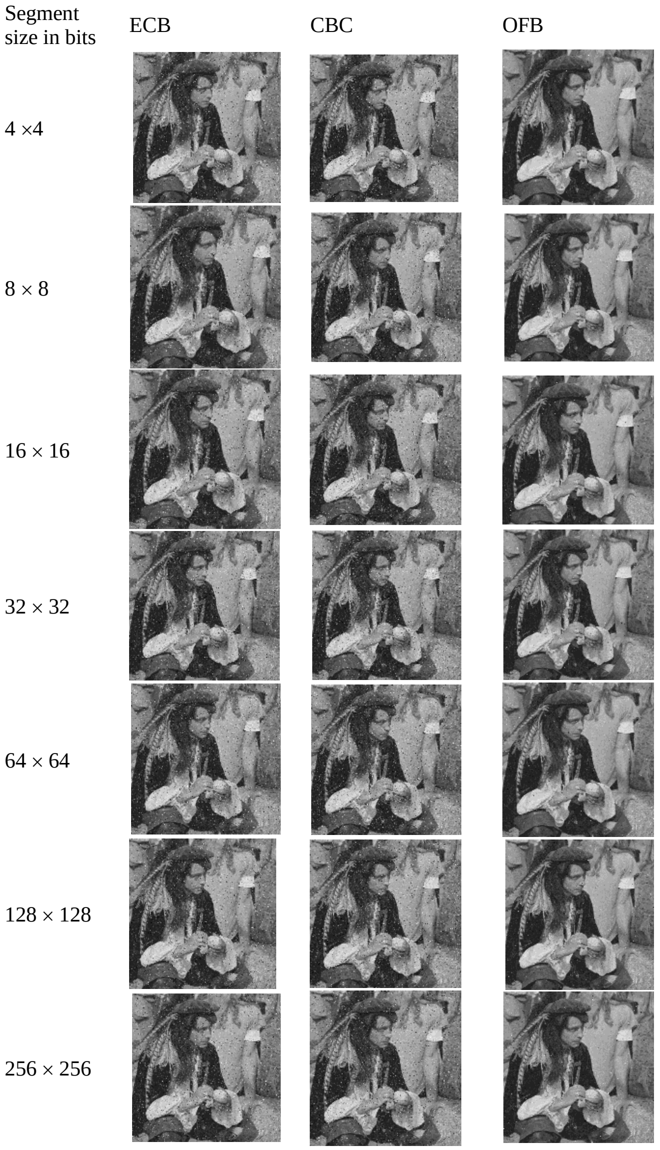

Fig. 4. Deciphered Pirate Images of the Proposed 2D Discretized CSM Cipher with the OFB and CBC with Various Segment Sizes and SNR=5dB.

TABLE IV. NUMERICAL PSNR VALUES OF THE 2D DISCRETIZED CSM IMAGE CIPHER, AND THE PROPOSED 2D DISCRETIZED CSM CIPHER WITH THE OFB AND CBC AND VARIOUS SEGMENT SIZES

Segment size in bits	**ECB**	**CBC**	**OFB**
4 ×4	20.3094	20.5365	29.4117
8 × 8	21.3683	20.6225	29.2111
16 × 16	21.4050	20.6223	29.1333
32 × 32	21.1286	20.5498	29.2305
64 × 64	21.1369	20.4960	29.5665
32 × 128	21.2714	20.8906	28.9257
256 × 256	21.3248	21.3151	29.4045

TABLE V. NUMERICAL CC VALUES OF THE 2D DISCRETIZED CSM IMAGE CIPHER, AND THE PROPOSED 2D DISCRETIZED CSM CIPHER WITH THE OFB AND CBC AND VARIOUS SEGMENT SIZES

Segment size in bits	**ECB**	**CBC**	**OFB**
4 ×4	0.9043	0.8862	0.9842
8 × 8	0.9057	0.8894	0.9834
16 × 16	0.9066	0.8892	0.9831
32 × 32	0.9002	0.8868	0.9836
64 × 64	0.9005	0.8856	0.9848
32 × 128	0.9036	0.8953	0.9824
256 × 256	0.9044	0.9042	0.9842

Also, the proposed 2D discretized CSM cipher with the OFB is more resistant to noise than the proposed 2D discretized CSM cipher with the ECB and CBC. Finally, it can be confirmed and ensured that the proposed 2D discretized CSM cipher with the OFB can provide a better trade-off among the security level and noise immunity.

VII. CONCLUSION

This paper introduces a 2D discretized CSM cipher with the ECB, OFB and CBC that depends on dividing the plainimage to be enciphered into segments and enciphering each segment with the 2D discretized CSM cipher with the ECB, OFB and CBC. The proposed 2D discretized CSM cipher with the OFB provides a better trade-off among the high noise resistivity and high security level. The tests demonstrated that the 2D discretized CSM cipher with the OFB and CBC also achieve a uniform histogram distribution that cannot be achieved using the proposed 2D discretized CSM cipher with the ECB. The 2D discretized CSM is compared in different modes of operation. The outcomes demonstrated that the proposed 2D discretized CSM with the OFB and CBC has a high security. Finally, the proposed 2D discretized CSM cipher with the OFB has good noise immunity than the proposed 2D discretized CSM cipher with the ECB and CBC.

ACKNOWLEDGMENT

This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

REFERENCES

[1] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-sayed, M. A. AlZain, J. F. Al-Amri, and F. E. Abd El-Samie, "Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications," IEEE Access, vol. 8, pp. 103200-103218, 2020.

[2] O. S. Faragallah, A. I. Sallam and H. S. El-Sayed, "Utilization of HEVC ChaCha20-based selective encryption for secure telehealth video conferencing," Computers, Materials & Continua, vol. 70, pp. 831-845, 2022.

[3] O. S. Faragallah, H. S. El-sayed, A. Afifi, W. El-Shafai, "Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform," Optics and Lasers in Engineering, vol. 137, 106333, 2021.

[4] C. E. Shannon, "Communication theory of secrecy system," Bell Syst. Tech. J., vol. 28, pp. 656–715, 1949.

[5] Z. Liu, C. Guo, J. Tan, W. Liu, J. Wu, Q. Wu, L. Pan, S. Liu, "Securing color image by using phase-only encoding in Fresnel domains," Opt. and Lasers in Eng., vol. 68, pp. 87-92, 2015.

[6] X. W. Li , Q. Wang , S. Kim, and I. Lee , "Encrypting 2D/3D image using improved lensless integral imaging in Fresnel domain," Opt. Commun., vol. 381, pp. 260-270, 2016.

[7] [19] S. holami, K. Jaferzadeh, and S. Shin, "An efficient image-based verification scheme by fusion of double random phase encoding and dynamic chaotic map," *Multimedia Tools and Applications*, vol. 78, pp. 25001–25018, 2019.

[8] E. Alvarez, A. Fernández, P. García, J. Jiménez, and A.Marcano, "A new approach to chaotic encryption" Physics Letters A, vol. 26, pp. 373-375, 1999.

[9] O. S. Faragallah, A. Afifi, I. F. Elashry, E. A. Naeem H. M. El-Hoseny, H. S. El-sayed, and A. M. Abbas, "Efficient optical double image cryptosystem using chaotic mapping-based Fresnel transform," Optical and Quantum Electronics, vol. 53, pp. 1-26, 2021.

[10] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-Sine map," Information Sciences, vol. 339, pp. 237-253, 2016.

[11] K. Wang,W. Pei, and L. Zou "Security of public key encryption technique based on multiple chaotic system" Physics Letters A, vol. 360, pp. 259-262, 2006.

[12] I. F. Elashry, W. El-Shafai, E. S. Hasan, S. El-Rabaie, A. M. Abbas, F. E. Abd El-Samie, H. S. El-sayed, and O. S. Faragallah, "Efficient chaotic-based image cryptosystem with different modes of operation," Multimedia Tools and Applications, vol. 79, pp. 20665-20687, 2020.

[13] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," Multimed. Tools Appl., vol. 75, pp. 6303-6319, 2016.

[14] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," Multidim. Syst. Sign. Process., vol. 30, no. 2, pp. 943–961, 2019.

[15] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," Multimed. Tools Appl., vol. 78, pp. 22023-22043, 2019.

[16] H. Chen, C. Tanougast, Z. Liu, W. Blondel, and B. Hao, "Optical hyperspectral image encryption based on improved Chirikov mapping and gyrator transform," Optics and Lasers in Engineering, vol. 107, pp. 62-70, 2018.

[17] G. Hu, D. Xiao, Y. Zhang, and T. Xiang, "An efficient chaotic image cipher with dynamic lookup table driven bit-level permutation strategy," Nonlinear Dynamics, vol. 87, no. 2, pp. 1359-1375, 2017.

[18] J. Thomas, "Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks," International Journal of Business Management, vol. 13, no. 6, pp. 1-24, 2018.

[19] D. Zhang, "Big data security and privacy protection," Proc. of 8th IEEE International Conference on Management and Computer Science (ICMCS 2018), pp. 275-278, Atlantis Press, October 2018.

[20] A. Belazi, M. Khan, A. A. Abd El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," Nonlinear Dynamics, vol. 87, no. 1, pp. 337-361, 2017.

[21] S. Lian, G. Sun, and Z. Wang, "A block cipher based on a suitable use of chaotic Standard map," Chaos, Solutions and Fractals, vol. 26, pp. 117-129, 2005.

[22] G. Hu, D. Xiao, Y. Zhang and T. Xiang, "An efficient chaotic image cipher with dynamic lookup table driven bit-level permutation strategy," Nonlinear Dynamics, vol. 87, no. 2, pp. 1359-1375, 2017.

[23] K. Wong, B. Kwok, and W. Law W, "A Fast Image Encryption Scheme based on Chaotic Standard Map," Phys. Lett A, vol. 37, pp. 112-117, 2007.

[24] O. S. Faragallah, A. I. Sallam and H. S. El-Sayed, "Visual protection using RC5 selective encryption in telemedicine," Intelligent Automation & Soft Computing, vol. 31, pp. 1717-190, 2022.

[25] J. Kohl, "The use of encryption in Kerberos for network authentication," Proceedings, Crypto-89, Springer-Verlag, 1989.

[26] M. Dworkin, Recommendation for block cipher modes of operation methods and techniques, NIST Special Publication 800-38A, 2001.

[27] B. Stoyanov and G. Nedzhibov, "Symmetric key encryption based on rotation-translation equation," Symmetry, vol. 12, pp. 1-12, 2020.

[28] A. Arab, M. J. Rostami and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," The Journal of Supercomputing, vol. 75, pp. 6663–6682, 2019.

[29] X. J. Tong and M. G. Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically, IVC, vol. 26, pp. 843-850, 2008.

[30] M. H. Abood, "An efficient 3DV frame cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), pp. 86-90, 2017.

[31] A. Abukari, E. Bankas, and M. Iddrisu, "A secured video conferencing system architecture using a hybrid of two homomorphic encryption schemes: a case of zoom," International Journal of Engineering Research & Technology (IJERT), vol. 9, pp. 237-240, 2020.

[32] O. S. Faragallah, H. S. El-sayed, A. Afifi, and S. F. El-Zoghdy, "Small details gray scale image encryption using RC6 block cipher," wireless Personal Communications, vol. 118, no. 2, pp. 1559-1589, 2021.

[33] O. S. Faragallah, M. A. AlZain, H. S. El-sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem, and B. Soh, "Secure color image cryptosystem based on chaotic logistic in the FrFT domain," Multimedia Tools and Applications, vol. 79, pp. 2495-2519, 2020.

[34] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-sayed, E. A. Naeem, M. A. AlZain, J. F. Al-Amri, B. Soh, and F. E. Abd El-Samie, "Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications," IEEE Access, vol. 8, pp. 42491-42503, 2020.

[35] Z. Xiong, K. Ramchandran, M. T. Orchard, and Ya-Qin Zhang, "A Comparative study of DCT- and wavelet-based image coding," IEEE transactions on circuits and systems for video technology, vol. 9(5), pp. 352-367, August 1999.

[36] O. S. Faragallah, W. El-Shafai, A. Afifi, I. Elashry, M. A. AlZain, J. F. Al-Amri, B. Soh, H. M. El-Hoseny, H. S. El-Sayed, and F. E.Abd El-Samie, "Efficient three-dimensional video cybersecurity framework based on double random phase encoding," *Intelligent Automation & Soft Computing*, vol. 28, pp. 353-367, 2021.

[37] A. Sallam, E. EL-Rabaie, and O. S. Faragallah,, "HEVC selective encryption using RC6 block cipher technique," IEEE Transactions on Multimedia, vol. 20, no. 7, pp. 1636-1644, 2018.

[38] A. M. Hemdan, O. S. Faragallah, O. Elshakankiry, and A. Elmhalaway, "A fast hybrid image cryptosystem based on random generator and modified logistic map," Multimedia Tools and Applications, vol. 78, no. 12, pp. 16177-16193, 2019.

[39] S. Sun, "A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling," IEEE Photonics Journal, vol. 10, pp. 1-14, 2018.

[40] O. S. Faragallah, W. El-Shafai, A. I. Sallam, I. Elashry, E. M. EL-Rabaie, A. Afifi, M. A. AlZain, J. F. Al-Amri, F. E. Abd El-Samie, and H. S. El-sayed, "Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication," Journal of Ambient Intelligence and Humanized Computing, vol. 13, pp. 1215-1239, 2022.

[41] G. Hu, D. Xiao, Y. Zhang, and T. Xiang, "An efficient chaotic image cipher with dynamic lookup table driven bit-level permutation strategy," Nonlinear Dynamics, vol. 87, pp. 1359-1375, 2017.

[42] O. S. Faragallah, A. Afifi, H. S. El-sayed, M. A. AlZain, J. F. Al-Amri, F. E. Abd El-Samie, and W. El-Shafai, "Efficient HEVC integrity verification scheme for multimedia cybersecurity applications," IEEE Access, vol. 8, pp. 154112-154135, 2020.