

Efficient Image Cipher Based on Baker Map in the Discrete Cosine Transform

Hesham Alhumyani

Computer Engineering Department, Taif University, Taif, Saudi Arabia

E-mail: h.alhumyani@tu.edu.sa

Abstract: *This paper presents an efficient image cipher based on applying the chaotic Baker Map (BM) in the Discrete Cosine Transform (DCT). The encryption module of the proposed DCT-based BM image cipher employs a DCT on the original plain-image then, the DCT coefficients of the plain-image are shuffled with the BM. Finally, the inverse DCT is applied to the shuffled plain-image DCT coefficients to obtain the final cipher-image. The decryption module of the proposed DCT-based BM image cipher employs a DCT on the input cipher-image then, the DCT coefficients of the cipher-image are inversely shuffled with the BM. Finally, the inverse DCT is applied to the inversely shuffled cipher-image DCT coefficients to obtain the original plain-image. A set of experimental tests are performed to test the validity of the proposed DCT-based BM image cipher and the performed tests demonstrated the superiority of the proposed DCT-based BM image cipher in terms of statistical, differential, sensitivity and noise immunity.*

Keywords: *Image-encryption, Baker map, DCT.*

1. Introduction

In the last decade, digital images production and sharing has been massively growing due to the advancement of networks and communication technology. Many potential applications of digital images such as military, medical, properties monitoring can be vulnerable to security attacks and leakage. Therefore, image encryption algorithms are a key solution for the issues of privacy and security in order to preserve confidentiality and integrity [1-3]. Different from text data, image data are bulky due to the redundancy and high correlation, which means that traditional text encryption algorithms are not appropriate when dealing with images. To mitigate this issue, a new class of encryption based on nonlinear theories have emerged. Chaotic based encryption is one of the nonlinear theories that has been used recently in image encryption, which is known to be secure and efficient [4-8]. Two main properties make chaotic based system good candidate for image encryption – initial condition

sensitivity and parameters sensitivity. Initial condition sensitivity defines the uncorrelation between two close points when applying chaotic map while the parameters sensitivity defines the instantaneous change of the map properties due to the parameter perturbation. As a matter of fact, these random behavior permutations using chaotic based encryption meet the requirement of confusion and diffusion mentioned in Shannon theory [9]. Moreover, the hardware and software implementation for chaotic systems is simple compared to other crypto systems that result in high encryption rates. As a result, chaotic based system has been one of the hot topics in cryptology [10-12].

Many chaos-based image encryption works has been presented in the literature [13-17]. In [18], an image encryption based on chaotic tent map has been presented. They use the chaotic tent map for generating chaotic key stream and perform a simple exclusive-or operation with the plain-image. However, this crypto system focuses only on applying diffusion of each pixel individually without confusion and which does not take into consideration the difference between gray and color images. In [19], an Image encryption using two chaotic logistic map and external 80-bit secret key has been proposed. In their encryption scheme, eight different operations have been used to encrypt a specific pixel that is determined from the logistic map. For further security, the secret key is updated after each block of the image where each block contains 16 pixels. The author of [20] have proposed an image encryption using 2D Baker's map by applying permutation first to the plain image through a sequence of pseudo random number as an outcome from the 2D Baker's map and then simple diffusion operation is applied based on exclusive-or operation. They used two different secret keys for permutation and diffusion. Due to the vulnerability of using single chaotic map and its limited range, the authors of [21] proposed a double chaotic system based on baker and logistics map. They used 2D Baker map to control the parameters and states of the logistic map. This results in periodic changing of the logistic map parameters and states where randomness and unpredictability can be obtained. In [22], image encryption based on baker map in the frequency domain DCT (Discrete Cosine Transform) has been proposed. Their work applies confusion using baker map and diffusion through exclusive-or operation on stream cipher. In this paper, we propose an efficient block image cryptosystem based on applying the chaotic baker mapping in the discrete cosine transform domain. The purpose of this work is to provide a comprehensive study of encryption and decryption scheme, which are studied and investigated taking into consideration several security performance metrics like statistical, sensitivity and differential tests. In [23], authors proposed a hybrid encryption-compression method based on multiple chaotic maps and Galois field. Experimental tests ensured that the proposed method improved the security of encrypted data. In [24], authors proposed a secret image sharing using XOR with arithmetic operations that upgrade traditional secret image sharing approaches performance. This proposed method conserved the fault tolerance feature, which has an impact role in image sharing. In [25], authors proposed a secret image enhanced sharing using visual cryptography for hiding large amount of secrets without any loss of information, confidentiality and data integrity. The proposed method confirmed privacy, security, confidentiality and integrity. In [26], authors

studied a large family of ciphers derivable from the DES and having an endowment to thwart differential and some fault-injection attacks. Experimental tests demonstrated that they could possess good resistance against several attack types. In [27] authors presented a Secured Document Sharing Using Visual Cryptography (SDSUVC) for achieving data privacy in a cloud computing model. Experiments demonstrated that the SDSUVC ensured data confidentiality and security along with integrity and reputation. In [28], authors proposed a multi-stage encoding method for multiple audio objects based on based on intra-object sparsity. Evaluations validated that the proposed encoding method achieved scalable transmission while keeping perceptual quality of each audio object. In [29] authors extended the analysis of the modified Hill cipher by considering a plain text of any size. The permutation, the interlacing and the iteration introduced in this analysis are found to cause diffusion and confusion efficiently. The paper rest is arranged as follows. Section 2 overviews and presents the utilized tools in the work like the discrete cosine transform and the 2D chaotic baker mapping. Section 3 gives the details of encryption/decryption procedures for the proposed DCT-based baker mapping image cryptosystem. Section 4 examines and discusses the experimental test results for the proposed DCT-based baker mapping image cryptosystem including the most important ones like statistical, sensitivity, and differential tests. Finally, Section 5 concludes the paper.

2. Fundamental tools

In this section, we present and overview the utilized tools employed in the proposed DCT-based baker mapping image cryptosystem. These tools include both the discrete cosine transform and the 2D chaotic baker mapping.

2.1. DCT

The discrete cosine transform represents a finite data set in the form of summation of cosine functions with varying frequencies. It is one of the Fourier transforms that uses real values with cosine functions to transform images from time domain to frequency domain. The main goal of DCT for images is to remove the redundancy among the correlated pixels that results in uncorrelated coefficients that can be processed through any operations independently. Moreover, the DCT is known of its energy compaction when dealing with high correlated images where it can discard those small coefficients values and can enable to reconstruct images without distortion. One of the main advantages of using the DCT in cryptography is to provide additional transformation operations through transforming pixels values into coefficients instead of dealing directly with the individual pixels. This cooperates in adding more security when dealing with these transformed operations that are able deviates attackers.

The 2-Dimensional Discrete Cosine Transform (2D-DCT) can be mathematically expressed as [22]

$$(1) \quad C(u, v) = \frac{2}{N} \alpha(u) \alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos \left[\frac{\pi(2x+1)u}{2N} \right] \cos \left[\frac{\pi(2y+1)v}{2N} \right].$$

The 2-Dimensional Inverse Discrete Cosine Transform (2D-IDCT) can be also mathematically expressed as [22]

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

where

$$(3) \quad \alpha(u) = \alpha(v) = \begin{cases} 1/\sqrt{2} & \text{if } u = v = 0, \\ 1 & \text{otherwise.} \end{cases}$$

2.2. Baker map

Baker map is one of the chaotic maps family that gives randomization by producing a set of sequenced pseudo-random numbers that results in an efficient crypto system. The Baker map (B) can be defined as

$$(4) \quad \begin{aligned} B(x, y) &= (2x, y/2) \quad \text{when } 0 \leq x < 1/2, \\ B(x, y) &= (2x-1, y/2+1/2) \quad \text{when } 1/2 \leq x \leq 1. \end{aligned}$$

The Baker map is classified into two types: generalized and discretized map. In generalized baker map, rather than dividing the square matrix into two equally halves which is unpractical in randomization as illustrated in Fig. 1.

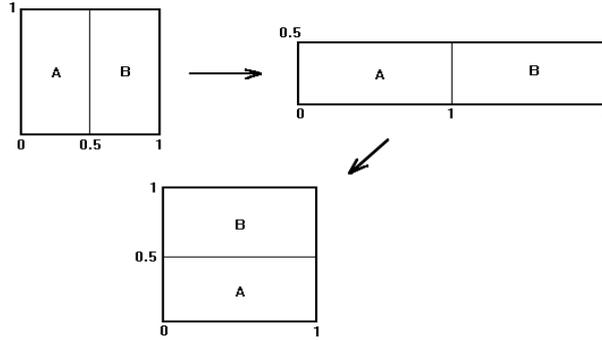


Fig. 1. Standard Baker map

The square matrix is divided into k vertical rectangles where k represents the secret key elements. As seen in Fig. 2, the square array is split into a number of k vertical rectangles $[X_{i-1}, X_i) \times [0, 1)$, $i = 1, \dots, k$, $X_i = z_1 + \dots + z_{i-1}$, such that $z_1 + \dots + z_k = 1$. The location of the i -th rectangle can be found by $X_i = z_1 + \dots + z_{i-1}$. Therefore, each rectangle is widened horizontally by the factor of $1/z_i$. Also, all rectangles are contracted vertically and scaled by a scale of p_i . In discretized baker map, each element of the square matrix needs to be changed into different position in a bijective manner. The Discretized Baker Map (DBM) can be expressed as $\text{DBM}_{(n_1, n_2, \dots, n_k)}(x, y)$ where (n_1, n_2, \dots, n_k) represents a set of k integers that divide N in which $N_i = n_1 + \dots + n_i$ (Fig. 3). And as a result, the pixel with indices (x, y) with $N_i \leq x < N_i + n_i$ and $0 \leq y < N$ is transformed to the position according to [4]:

$$(5) \quad \text{DBM}_{(n_1, \dots, n_k)}(x, y) = \left[\frac{N}{n_i} (x - N_i) + y \right] \bmod \left(\frac{N}{n_i} \right), \frac{n_i}{N} \left(y - y \bmod \left(\frac{N}{n_i} \right) \right) + N_i.$$

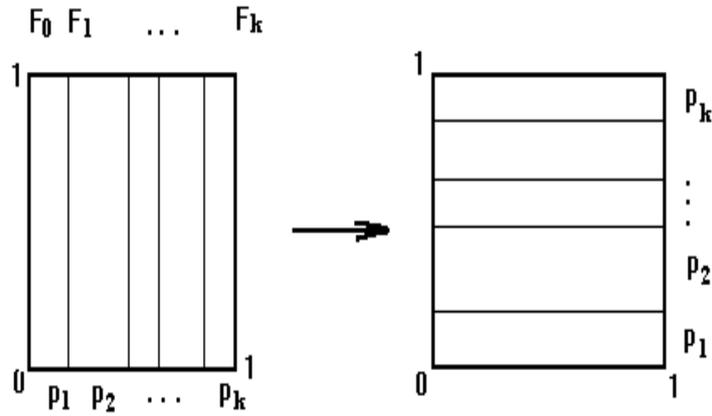


Fig. 2. Generalized Baker map

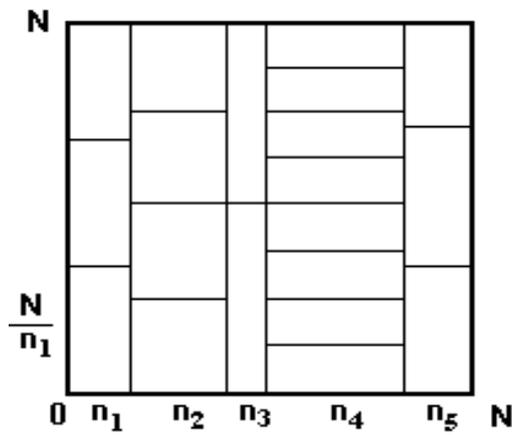


Fig. 3. Discretized Baker map

3. The proposed DCT-based Baker mapping image cryptosystem

The proposed DCT-based Baker mapping image cryptosystem includes two procedures that are encryption and decryption procedures.

3.1. Encryption procedure

The encryption procedure is shown in Fig. 4 begins with applying the DCT transform to the input plain image which produces the DCT coefficients of the plain image. Then, the plain image DCT coefficients is transposed (permuted) using the baker mapping. Finally, transformation is applied using the inverse DCT to produce the final cipher image.

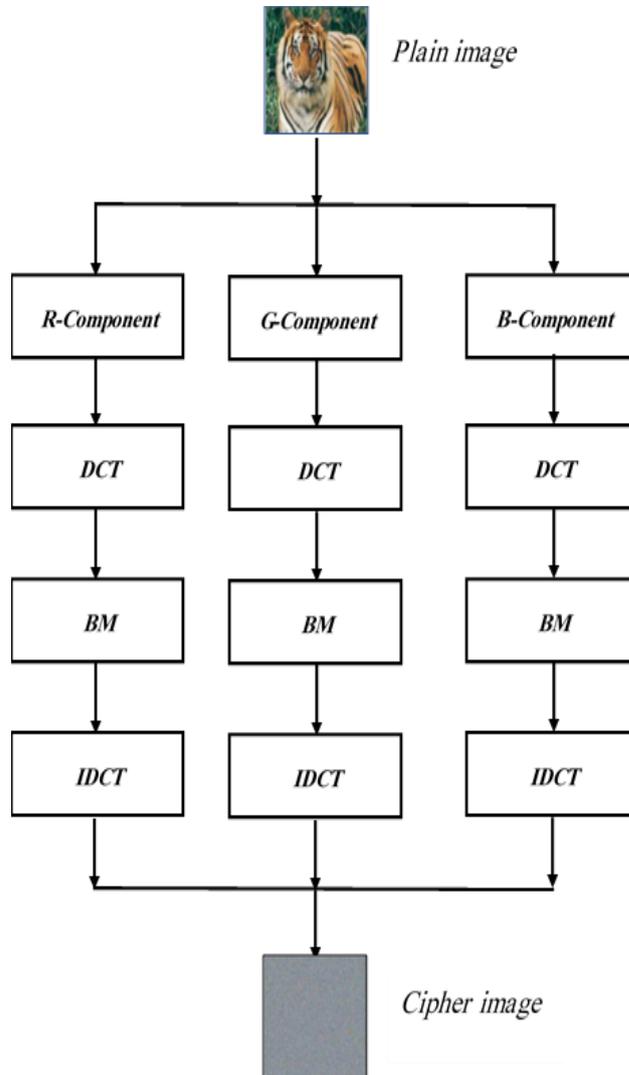


Fig. 4. Block-diagram for Encryption module of the proposed DCT-based Baker image cipher

3.2. Decryption procedure

The decryption procedure is shown in Fig. 5 is the inverse of encryption procedure. It begins with applying the DCT transform to the input cipher image, which produces the cipher image DCT coefficients. Then, the cipher image DCT coefficients are transposed (permuted) by applying the inverse baker mapping. Finally, transformation is applied using the inverse DCT to produce the plain image.

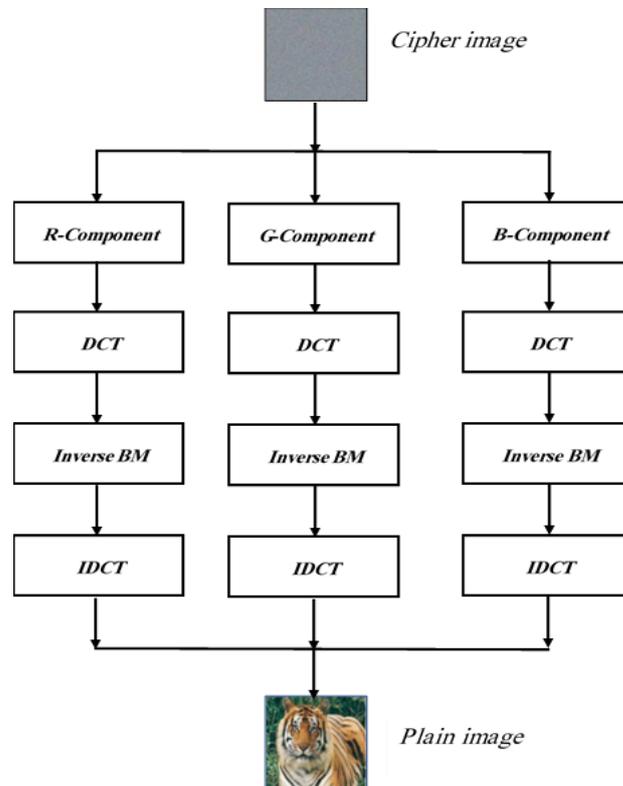


Fig. 5. Block-diagram for Decryption module of the proposed DCT-based Baker image cipher

4. Experimental tests and discussions

In this section, we have conducted a series of tests to examine the efficiency of the proposed DCT-based baker mapping image cryptosystem. In addition, the proposed DCT-based baker mapping image cryptosystem is compared with the baker map-based image cryptosystem. The comparison is conducted to show the effect of several encryption key performance metrics such as statistical, entropy and differential tests, visual inspecting, and noise tests. During our experiments, we have utilized three 256×256 color images as original color plain-images. These color plain-images are Fruits, and Color as illustrated in Fig. 6.

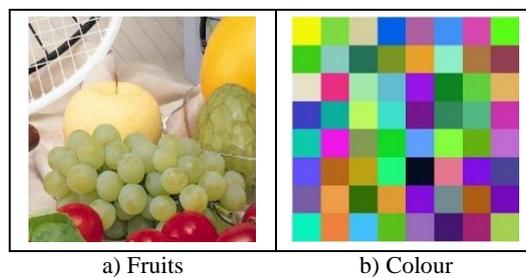


Fig. 6. The utilized Test color images

4.1. Visual inspecting results

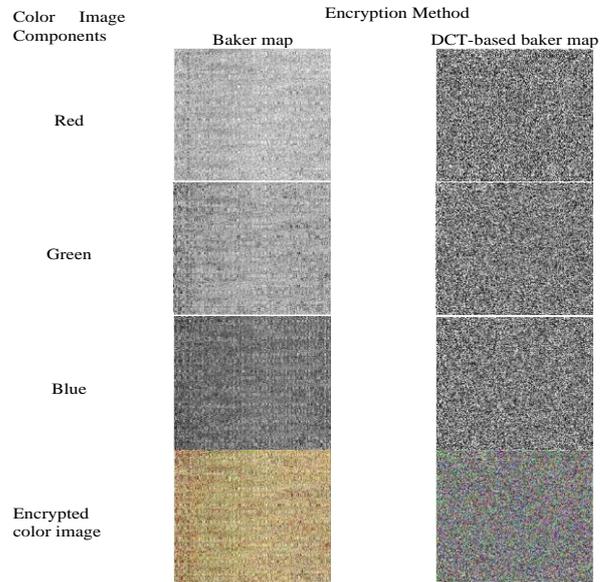


Fig. 7. The visual encryption results using baker mapping and the proposed DCT-based baker mapping for color Fruits image

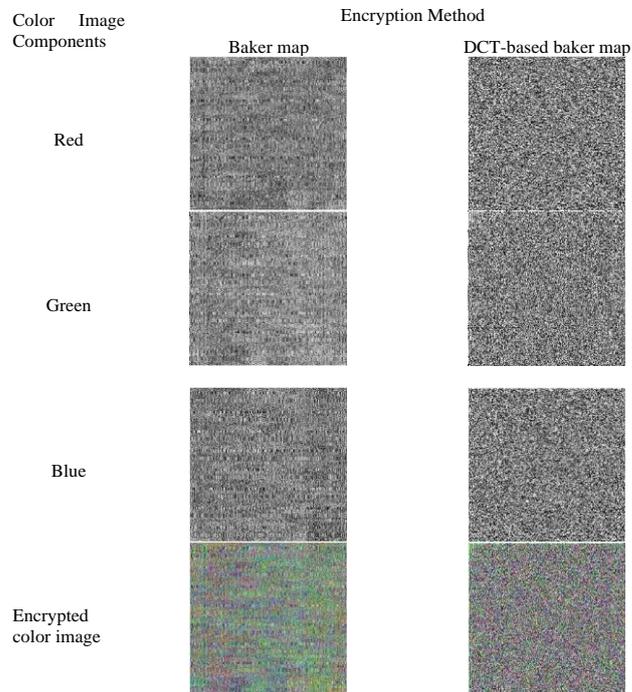


Fig. 8. The visual encryption results using baker mapping and the proposed DCT-based baker mapping for color Colour image

The visually inspected encryption results of color Fruits, Color, and House images using the proposed DCT-based baker mapping image and the chaotic baker mapping cryptosystems are illustrated in Figs 7-8, respectively. From the obtained results, it is clear that all encrypted color images are completely different from their corresponding color plain-images. Also, the visually inspected encryption results of color Fruits, Color, and House ensured and confirmed the superiority of the proposed DCT-based baker mapping image cryptosystem in omitting and removing all the attributes of the color plain-images.

4.2. Histogram testing

For a perfect color image cryptosystem, the cipher must result in a cipher-image whose red, green and blue histograms are uniformly distributed and totally distinct compared with their respected red, green and blue histograms of the color plain-images. The histogram results of plain/cipher red, green and blue components of color Fruits, Color, and House images are shown in Figs 9-10. The histogram results clearly show that the standard baker map encryption does not alter the histograms of the ciphered red, green and blue components of color Fruits, Color, and House images. On the other hand, the histogram results of the proposed DCT-based baker map encryption demonstrate that the red, green and blue components histograms of the resulted cipher-images are totally different compared with red, green and blue components histograms of their corresponding plain-images.

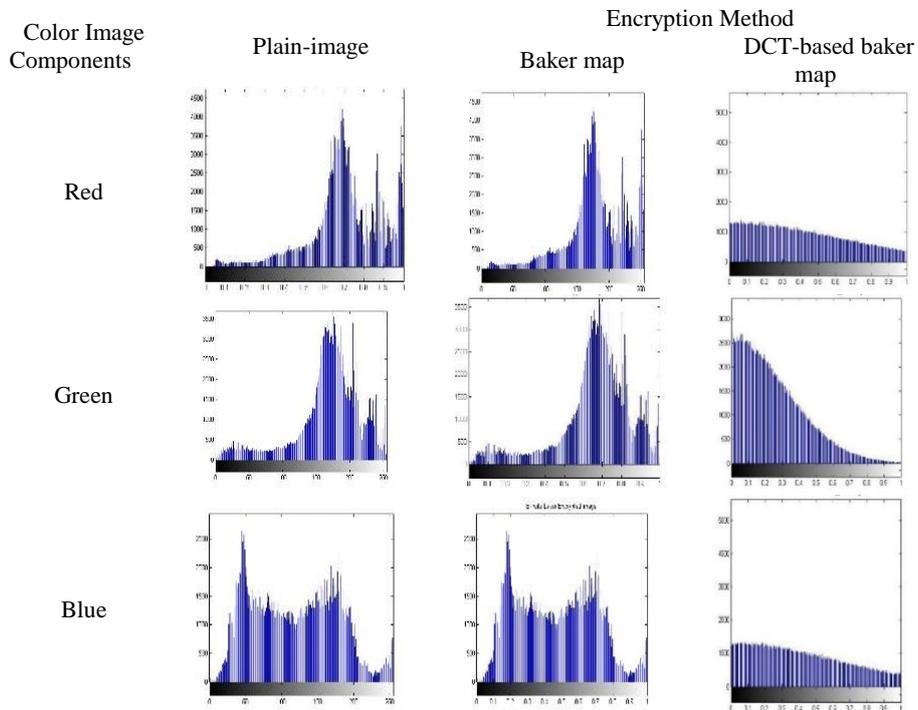


Fig. 9. Histogram of Red, Green and Blue plain/cipher images using baker mapping and the proposed DCT-based baker mapping for color Fruits image

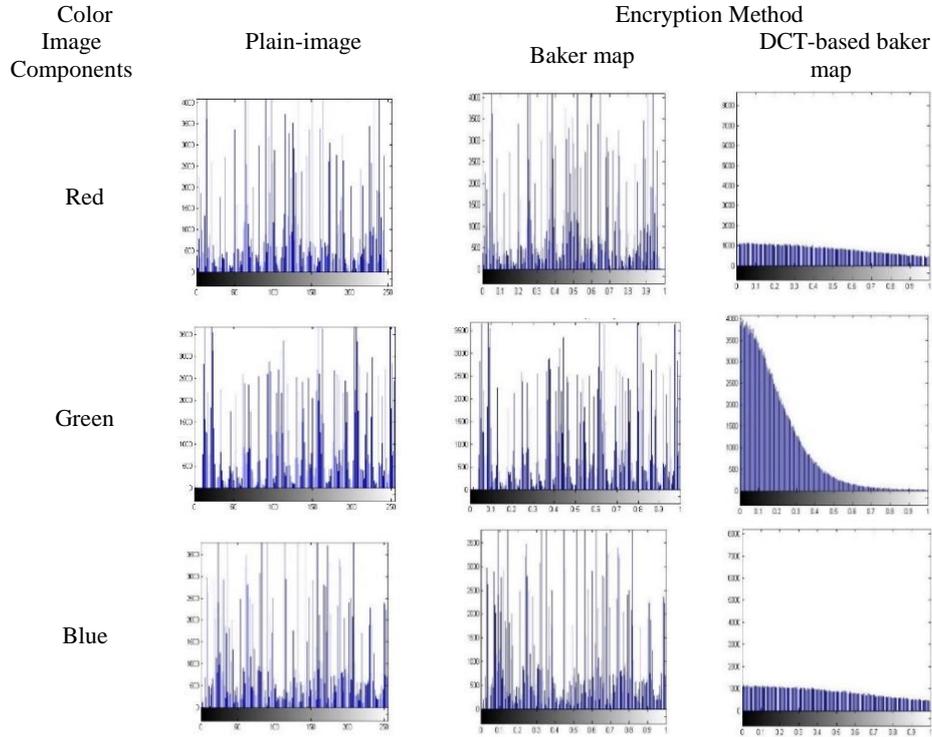


Fig. 10. Histogram of Red, Green and Blue plain/cipher images using baker mapping and the proposed DCT-based baker mapping for color Colour image

4.3. Correlation coefficient tests

A good image encryption produces a very small correlation value near the optimal value of zero. Here, the correlation coefficient measure is employed to investigate the relationship between the plain-image and the produced cipher-image using both the baker map and DCT-based baker encryption. The correlation coefficient r_{xy} is utilized to estimate the correlation between the color plain-image **PI** and its corresponding cipher-image **CI** and can be mathematically evaluated using the next equation [30-32]:

$$(6) \quad r_{xy} = \frac{E\{(\mathbf{CI}-E(\mathbf{CI})) \cdot (\mathbf{PI}-E(\mathbf{PI}))\}}{\sqrt{E\{[\mathbf{CI}-E(\mathbf{CI})]^2\}} \sqrt{E\{[\mathbf{PI}-E(\mathbf{PI})]^2\}}}$$

Table 1 shows the correlation coefficient estimations between **PI** red, green and blue color components and their corresponding **CI** red, green and blue components using both the baker map and DCT-based baker encryption. It is obvious from Table 1 that the obtained correlation coefficients are approximately near to the ideal value of zero. These results validate and verify the proposed DCT-based baker encryption in terms of the obtained correlation coefficients that are closely reaching the optimal zero value.

Table 1. Correlation coefficients between plain/cipher images Red, Green and Blue components using baker mapping and the proposed DCT-based baker mapping for color Fruits and Colour images

Image	Encryption method					
	Baker			DCT-based Baker		
	<i>R</i>	<i>G</i>	<i>B</i>	<i>R</i>	<i>G</i>	<i>B</i>
Fruits	-0.0140	-0.0245	-0.0413	0.0120	0.0055	0.0321
Colour map	0.0115	0.0016	0.0188	-0.0065	0.0272	0.0037

4.4. Information entropy analysis

The information entropy analysis is conducted to estimate the information amount contained in the entire the red, green and blue components of the color cipher-image. The information entropy amount is expressed in bits and has an ideal value of 8. It can be mathematically formulated as given by the next equation:

$$(7) \quad \text{Entropy}(V) = \sum_{i=1}^{2^N-1} P(V_i) \log_2 \frac{1}{P(V_i)},$$

where $\text{Entropy}(V)$ and $P(V_i)$ are the entropy and the symbol V_i occurrence probability. Table 2 shows the entropy estimations in bits of **PI** Red, Green and Blue color components and their corresponding **CI** Red, Green and Blue components using both the baker map and DCT-based baker encryption. It is obvious from Table 2 that the obtained correlation coefficients are approximately near to the ideal value of 8.

Table 2. Entropy of plain/cipher images Red, Green and Blue components using baker mapping and the proposed DCT-based baker mapping for color Fruits and Colour images

Image	Color Plain-image components			Encryption method					
	<i>R</i>	<i>G</i>	<i>B</i>	Baker			DCT-based Baker		
				<i>R</i>	<i>G</i>	<i>B</i>	<i>R</i>	<i>G</i>	<i>B</i>
Fruits	7.0556	7.3527	7.7134	7.0556	7.3527	7.7134	7.4559	7.3784	7.4608
Colour map	7.1556	7.3043	7.2917	7.1556	7.3043	7.2917	7.0425	6.9457	7.1115

4.5. Differential test

The differential test is carried to examine the effect of modifying one pixel in two plain-images and observing the impact of this change in their corresponding cipher-images. To fulfil such requirements, we utilize two estimations called the Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). The NPCR is mathematically expressed using the next equation as in [33-35]:

$$(8) \quad \text{NPCR}_{R,G,B}(\mathbf{CI}^1, \mathbf{CI}^2) = \frac{\sum_{ij} \text{DIF}_{R,G,B}(x_i, y_j)}{N} \times 100\%,$$

where N is total number of image pixels and $\text{DIF}_{R,G,B}(x_i, y_j)$ is mathematically expressed using the next equation as in [33-35]:

$$(9) \quad \text{DIF}_{R,G,B}(\mathbf{CI}^1, \mathbf{CI}^2) = \begin{cases} 0, & \mathbf{CI}_{R,G,B}^1(x_i, y_j) = \mathbf{CI}_{R,G,B}^2(x_i, y_j), \\ 1, & \mathbf{CI}_{R,G,B}^1(x_i, y_j) \neq \mathbf{CI}_{R,G,B}^2(x_i, y_j), \end{cases}$$

where $\mathbf{CI}_{R,G,B}^1(x_i, y_j)$ and $\mathbf{CI}_{R,G,B}^2(x_i, y_j)$ represent are the red, green and blue components of the two color cipher-images $\mathbf{CI}^1, \mathbf{CI}^2$.

The $UACI_{R,G,B}$ is mathematically expressed using the next equation as in [33-35]:

$$(10) \quad UACI_{R,G,B}(CI^1, CI^2) = \frac{1}{N} \left[\sum_{i,j} \frac{|CI^1_{R,G,B}(x_i, y_j) - CI^2_{R,G,B}(x_i, y_j)|}{255} \right] \times 100\%.$$

The obtained results for both NPCR and UACI are listed in Table 3. The achieved results prove and ensure the high sensitivity of the proposed DCT-baker image cryptosystem with respect to small changes like just one-pixel modification.

Table 3. The NPCR and UACI results of plain/cipher images Red, Green and Blue components using Baker mapping and the proposed DCT-based Baker mapping for color Fruits and Color images

Image		Encryption method					
		Baker			DCT-based Baker		
		<i>R</i>	<i>G</i>	<i>B</i>	<i>R</i>	<i>G</i>	<i>B</i>
Fruits	NPCR	100	99.9405	99.9996	100	100	100
	UACI	0	0	0	0	0	0
Colour map	NPCR	100	99.9996	100	100	100	100
	UACI	0	0	0	0	0	0

5. Conclusion

An efficient image cryptosystem based on employing the BM in DCT is presented in the present article. The proposed DCT-based image cipher is tested using a series of experimental tests such as visual, entropy, statistical, differential and noise immunity tests. The obtained results proved the efficiency of the proposed DCT-based BM image cipher against different types of attacks. Also, the results of noise immunity demonstrated that the proposed DCT-based BM image cipher is highly resistant against AWGN noise at different variations.

References

- Daemen, J., V. Rijmen. The Design of Rijndael: AES – the Advanced Encryption Standard. Springer Science & Business Media, 2013.
- Rivest, R. L. The RC5 Encryption Algorithm. – In: Proc. of 2nd International Workshop, Fast Software Encryption, Springer-Verlag, 1995, pp. 86-96.
- Rivest, R., M. Robshaw, R. Sidney, Y. L. Yin. The RC6 Block Cipher. – In: NIST AES Proposal, 1998.
- Fridrich, J. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. – Int. J. Bifurc. Chaos, Vol. **8**, 1998, pp. 1259-1284.
- Wang, X., L. Teng. An Image Blocks Encryption Algorithm Based on Spatiotemporal Chaos. – Nonlinear Dyn., Vol. **67**, 2011, pp. 365-371.
- Ye, G. D., K. W. Wong. An Efficient Chaotic Image Encryption Algorithm Based on a Generalized Arnold Map. – Nonlinear Dyn., Vol. **69**, 2012, pp. 2079-2087.
- Tong, Z. Novel Bilateral-Diffusion Image Encryption Algorithm with Compound Chaos and LFSR. – J. Imaging Sci., Vol. **60**, 2012, pp. 294-304.
- Wang, X., D. Lu. A Novel Image Encryption Algorithm Using Chaos and Reversible Cellular Automata. – Commun. Nonlinear Sci. Numer. Simul., Vol. **18**, 2013, pp. 3075-3085.
- Shannon, C. Communication Theory of Secrecy Systems. – Bell System Technical Journal, Vol. **28**, 1949, pp. 656-715.

10. T o n g, X. Design of an Image Encryption Scheme Based on a Multiple Chaotic Map. – Commun. Nonlinear Sci. Numer. Simul., Vol. **18**, 2013, pp. 1725-1733.
11. T o n g, X., Z. W a n g, M. Z h a n g. A New Algorithm of the Com-Bination of Image Compression and Encryption Technology Based on Cross Chaotic Map. – Nonlinear Dyn., Vol. **72**, 2013, pp. 229-241.
12. W a n g, X., K. G u o. A New Image Alternate Encryption Algorithm Based on Chaotic Map. – Nonlinear Dyn., Vol. **76**, 2014, pp. 1943-1950.
13. Y e, R., W. G u o. A Chaos-Based Image Encryption Scheme Using Multimodal Skew Tent Maps. – J. Emerg. Trends Comput. Inf. Sci., Vol. **4**, 2013, No 10.
14. Y e, R., W. Z h o u. A Chaos-Based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice. – Int. J. Comput. Netw. Inf. Secur., Vol. **4**, 2012, No 1, pp. 25-28.
15. K a n s o, A. Self-Shrinking Chaotic Stream Ciphers. – Commun. Nonlinear Sci. Numer. Simul., Vol. **16**, 2011, No 2, pp. 822-836.
16. A k h a v a n, A., A. S a m s u d i n, A. A k h s h a n i. A Symmetric Image Encryption Scheme Based on Combination of Nonlinear Chaotic Maps. – J. Frankl. Inst., Vol. **348**, 2011, No 8, pp. 1797-1813.
17. J a k i m o s k i, G., L. K o c a r e v et al. Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps. – IEEE Trans. Circuits Syst. I Fundam. Theory Appl., Vol. **48**, 2001, No 2, pp. 163-169.
18. L i, C., G. L u o, K. Q i n, C. L i. An Image Encryption Scheme Based on Chaotic Tent Map. – Nonlinear Dyn., Vol. **87**, 2017, No 1, pp. 127-133.
19. P a r e e k, N. K., V. P a t i d a r, K. K. S u d. Image Encryption Using Chaotic Logistic Map. – Image and Vision Computing, Vol. **24**, 2006, No 9, pp. 926-934.
20. M o n d a l, B., P. K u m a r, S. S i n g h. A Chaotic Permutation and Diffusion-Based Image Encryption Algorithm for Secure Communications. – Multimedia Tools and Applications, 2018. DOI:10.1007/s11042-018-6214-z.
21. L u o, Y., J. Y u, W. L a i, L. L i u. A Novel Chaotic Image Encryption Algorithm Based on Improved Baker Map and Logistic Map. – Multimedia Tools and Applications, 2019. DOI:10.1007/s11042-019-7453-3.
22. C h e n g, L. Z. On Computing the Two-Dimensional (2-D) Type IV Discrete Cosine Transform (2-D DCT-IV). – IEEE Signal Processing Letters, Vol. **8**, 2011, pp. 239-241.
23. P r a s a d, B., K. M i s h r a. A Combined Encryption Compression Scheme Using Chaotic Maps. – Cybernetics and Information Technologies, Vol. **13**, 2013, No 2, pp. 75-81.
24. V e r m a, M., R. R a n i m. Significant Secret Image Sharing Scheme Based on Boolean Operation. – Cybernetics and Information Technologies, Vol. **17**, 2017, No 2, pp. 134-150.
25. B r i n d h a, K., N. J e y a n t h i. Secret Image Enhanced Sharing Using Visual Cryptography. – Cybernetics and Information Technologies, Vol. **17**, 2017, No 3, pp. 128-139.
26. B o r i s s o v, Y., P. B o y v a l e n k o v, R. T s e n k o v. On a Linear Cryptanalysis of a Family of Modified DES Ciphers with Even Weight S-Boxes. – Cybernetics and Information Technologies, Vol. **16**, 2016, No 4, pp. 3-12.
27. B r i n d h a, K., N. J e y a n t h i. Secured Document Sharing Using Visual Cryptography in Cloud Data Storage. – Cybernetics and Information Technologies, Vol. **15**, 2015, No 4, pp. 111-123.
28. Y a n g, Z., M. J i a, W. W a n g, J. Z h a n g. Multi-Stage Encoding Scheme for Multiple Audio Objects Using Compressed Sensing. – Cybernetics and Information Technologies, Vol. **15**, 2015, No 6, pp. 135-146.
29. S a s t r y, V. U. K., N. R. S h a n k a r, S. D. B h a v a n i. A Large Block Cipher Involving Key Dependent Permutation, Interlacing and Iteration. – Cybernetics and Information Technologies, Vol. **13**, 2013, No 3, pp. 50-63.
30. P r i y a, R., R. V i d h y a p r i y a, K. S e i f e d i n e, D. R o b e r t a s, B. T o m a s. An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic-Tent Map. – Entropy, Vol. **21**, 2019, 656, pp. 1-17.
31. S a l l a m, A. I., M. E l-S a y e d, E l-R a b a i e, O. S. F a r a g a l l a h. CABAC-Based Selective Encryption for HEVC Using RC6 in Different Operation Modes. – Multimedia Tools and Applications, Vol. **77**, 2018, No 21, pp. 28395-28416.

32. Faragallah, O. S. Optical Double Color Image Encryption Scheme in the Fresnel-Based Hartley Domain Using Arnold Transform and Chaotic Logistic Adjusted Sine Phase Masks. – Optical and Quantum Electronics, Vol. **50**, 2018, No 3:118, pp. 1-27.
33. Sallam, A. I., M. El-Sayed, El-Rabaie, O. S. Faragallah. HEVC Selective Encryption Using RC6 Block Cipher Technique. – IEEE Transactions on Multimedia, Vol. **20**, 2018, No 7, pp. 1636-1644.
34. Faragallah, O. S., M. A. Alzain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naem, B. Soh. Block-Based Optical Color Image Encryption Based on Double Random Phase Encoding. – IEEE Access, Vol. **7**, 2018, pp. 4184-4194.
35. Hemdan, A. M., O. S. Faragallah, O. Elshakankiry, A. Elmhaway. A Fast Hybrid Image Cryptosystem Based on Random Generator and Modified Logistic Map. – Multimedia Tools and Applications, Vol. **78**, 2019, No 12, pp. 16177-16193.

Received: 28.11.2019; Second Version: 27.12.2019; Accepted: 06.01.2020 (fast track)