Performance analysis of gray code number system in image security

Akinbowale Nathaniel Babatunde[1*], Ebunayo Rachael Jimoh[2], Oladipupo Oshodi[1], Olujuwon Ayoseyi Alabi[3]

[1]Department of Computer Science, College of Communication and Information Technology, Kwara State University
P.M.B 1530, Malete, Kwara State, Nigeria

[2]Department of Physical and Mathematical Sciences, Faculty of Science, Crown Hill University
Ballah road, Eiyenkorin, Ilorin, Kwara State, Nigeria

[3]Department of Computer Science, Abo Akademi University
Tuomiokirkontori 3, 20500 Turku, Finland

How to cite: A. N. Babatunde, E. R. Jimoh, O. Oshodi, and O. A. Alabi, "Performance analysis of gray code number system in image security," *Jurnal Teknologi dan Sistem Komputer*, vol. 7 no. 4, pp. 141-146, 2019. doi: 10.14710/jtsiskom.7.4.2019.141-146, [Online].

Abstracts - The encryption of digital images has become essential since it is vulnerable to interception while being transmitted or stored. A new image encryption algorithm to address the security challenges of traditional image encryption algorithms is presented in this research. The proposed scheme transforms the pixel information of an original image by taking into consideration the pixel location such that two neighboring pixels are processed via two separate algorithms. The proposed scheme utilized the Gray code number system. The experimental results and comparison shows the encrypted images were different from the original images. Also, pixel histogram revealed that the distribution of the plain images and their decrypted images have the same pixel histogram distributions, which means that there is a high correlation between the original images and decrypted images. The scheme also offers strong resistance to statistical attacks.

Keywords: Gray code number system; spatial domain; image encryption.

I. Introduction

A digital image can be defined as an m by n rectangular array of dots, where m is the number of rows, and n is the number of columns. In technical terms, a digital image P is a rectangular array of intensity values $\left(p_{i,j}\right)_{i,j=1}^{m,n}$. For gray-level images, the value $P_{i,j}$ is a single number, while for color images $P_{i,j}$ is a vector of three or more values. If the image is recorded in the RGB-model, each $P_{i,j}$ is a vector of three values, $p_{i,j}=\left(r_{i,j},g_{i,j},b_{i,j}\right)$. This denotes the amount of red, green and blue value at the point (i, j). The value $P_{i,j}$ gives the color information at the point (i, j). There are many formats for this. A digital image is made up of a raster of picture elements called pixels (Bitmaps). Each pixel is a very tiny square that is assigned a color and then arranged in a pattern to form the image. It has two properties, namely pixel location, and color. The resolution (finesess) of an image is the number of available pixels per unit area in the digital image [1], [2].

Recently, images have found widespread usage in many applications and fields, such as in the area of medicine, military, entertainment, art, education, and advertising due to its high information representation ability. Aside from the fact that images require the less cognitive load to understand, a digital image can produce at a glance information that can be spread across about ten pages in a book [3]. However, owing to the rapid developments in the efficient internet technologies and compression techniques the need for securing digital images during transmission and storage cannot be overemphasized [1], [4]-[7]. The main idea behind image security includes confidentiality, authentication, conditional access, integrity, content tracking, and copy control [7]-[9].

All digital system configurations depend so much on number systems [1], [10], [11]. There are majorly two number systems in the literature; the conventional or positional (Weighted Number System) and the unconventional or the non-positional (Unweighted Number System) number systems. Digital devices are mostly built around the weighted number systems (WNS) [1], [11]. The major problem with the WNS is in the carrying propagation chains in its operations, and to improve the performance of processors built around WNS in terms of speed and area cost. Hence, there is a need to eliminate the associated inherent carry propagation. Most unconventional number systems, such as residue number system, and gray code number systems, provide solutions to these problems.

Gray code number system is an encoding of number in which adjacent numbers have a single-digit differing by 1 [3]. The number system has the property that there is only one bit change between any two consecutive numbers. The numbers are arranged so that every transition from one value to the next value involves only one bit change. It is referred to as a mirrored binary number system because the first eight values can be

[*] Correspondence author (A. N. Babatunde)
Email: akinbowale.babatunde@kwasu.edu.ng

Submitted: 16 February 2019; Revised: 27 August 2019; Accepted: 5 September 2019; Published: 31 October 2019

compared with those of the last eight values but in reverse order. There are many types of Gray Code arithmetic; n-ary, balanced, monotonic, Beckett, and single-track Gray code number systems have been reported in the literature.

The n-ary Gray code number systems use non-Boolean arithmetic in its encodings. A special kind of n-ary gray code called the (n, k, p) gray code was proposed in [12]. This n-ary Gray code presents a new distant parameter p with the idea of the (n, k) Gray code. The new (n, k, p) Gray code changes as the estimations of the base n and the distant parameter p differ.

Gray code arithmetic has been reported to be efficient in its application in the area following areas in the literature; straight and rotational shaft position encoding systems, puzzle challenges solver, error corrections, genetic algorithms, protection of digital circuit designs, image processing, image stabilization, video processing, and scrambling [1], [3], [13]-[20]. Although the use of the Gray code number system can be applied in so many areas, its unweighted nature has made it is so unsuitable for arithmetic operations [21]-[23]. Various image encryption techniques have been reported in the literature.

Three types of encryption techniques exist; position permutation-based algorithm, value transformation-based algorithm, and hybrid substitution-based algorithm.Permutation-based algorithms rearrange image pixels using bits, pixels, or blockwise means, and transformation algorithms transform each pixel value with a new value. The hybrid substitution-based algorithm uses both permutation and transformation by combining them [1]. In [21]-[27] were reported for the position permutation-based algorithms, [28]-[30] have been reported for value transformation based algorithms while [12], [27]-[40] reported for hybrid substitution-based algorithm.

Researchers over the years have proposed various security measures, such as digital watermarking, encryption, compression, and steganography, to tackle this problem of insecurity image transmission and storage [5], [6], [8], [41]-[53]. All these methods are not efficient owing to their inability to encrypt images of m by n size [5], [6], and attain high degree encryption without pixel location permutation or scrambling [3].

This paper presents a scheme that encrypts and decrypts digital images of all sizes without positional scrambling. This proposed encoding methodology is designed to be able to transform the pixel values of an image without having to alter the pixel position (without scrambling). The proposed scheme, which utilizes the Gray code number system, will be demonstrated to efficiently secure digital images from unauthorized access during transmission and also retrieve the plain image without loss of any inherent information.

II. Research Methods

The primary aim of this paper is to analyze the performance of gray code arithmetic in image security. The work presents the implementation and security analysis of the algorithms presented in [1].

The algorithm was carried out in two phases. The first phase was designed to encode the binary representation of images to gray code values. G is the (n, k, p) gray code of k bits base-n nonnegative image X if the sequences are satisfied with $G=\left(C_p * X\right) mod\, n$. C_p is a constant for converting binary to gray-code. and n is the base. If $C_p=M_p$, then G will be (n, k) gray code. If $C_p=O_p$, then G will be (n, k, p) Gray code with distant parameter (p) of 2.

$$M_p=\begin{bmatrix}10000000\\11000000\\01100000\\00110000\\00011000\\00001100\\00000110\\00000011\end{bmatrix},\quad O_p=\begin{bmatrix}10000000\\01000000\\00100000\\10010000\\01001000\\00100100\\00010010\\00001001\end{bmatrix}$$

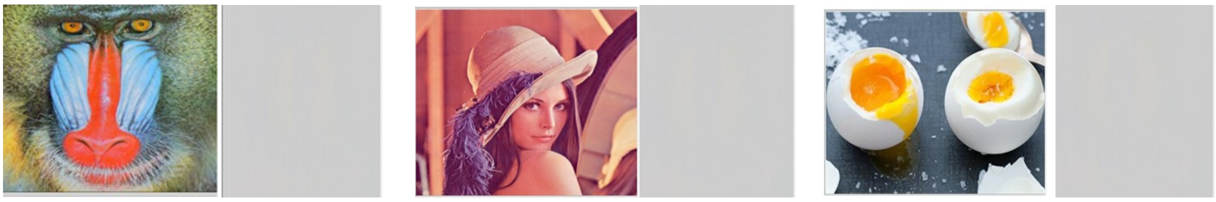
However, if p = 0 and k = 8, then the matrix can be shown as:

$$\begin{matrix}g_7\\g_6\\g_5\\g_4\\g_3\\g_2\\g_1\\g_0\end{matrix} = \begin{bmatrix}10000000\\11000000\\01100000\\00110000\\00011000\\00001100\\00000110\\00000011\end{bmatrix} \times \begin{matrix}x_7\\x_6\\x_5\\x_4\\x_3\\x_2\\x_1\\x_0\end{matrix}\; mod\, n$$

If p = 2, k = 8 and n = 2, then the matrix can be shown as:

$$\begin{matrix}g_7\\g_6\\g_5\\g_4\\g_3\\g_2\\g_1\\g_0\end{matrix} = \begin{bmatrix}10000000\\01000000\\00100000\\10010000\\01001000\\00100100\\00010010\\00001001\end{bmatrix} \times \begin{matrix}x_7\\x_6\\x_5\\x_4\\x_3\\x_2\\x_1\\x_0\end{matrix}\; mod\, 2$$

The second phase was used to encrypt the pixel values of m by n images such that two neighboring pixel values with the same RGB information will not have the same cipher information. For this, each pixel location is scanned. Based on the scan result, an algorithm is selected to encrypt the pixel location. There are four possible algorithms to be selected from using Eq. 1. If the result is 0, then an algorithm style is selected, but if it is 1, 2, or 3, then different unique algorithms are picked.



(a) Baboon (b) Lena (c) Eggs

Figure 1. Sample of original and encrypted images

$$Algorithm_{selected} = ((i * width\,length) + j) \bmod 4 \quad (1)$$

III. Results and discussion

The proposed scheme was analyzed using visual test, encoding and security analysis.

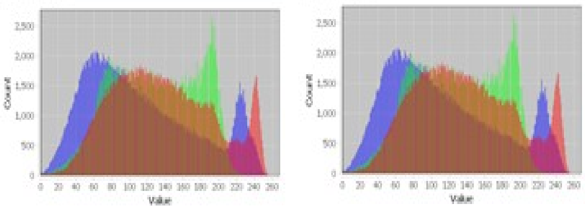
A. Visual Test

In all, three images of different sizes in colored format were used to test the developed system. Figure 1 shows the test results for the images; Baboon (512*512) in png format, Lena (512*512) in png format, and eggs (300*250) in jpg format. The visual test shows an absolute absence of resemblance among the pairs of images.

In a bid to prove that the decrypted image fully recovered the original image without any inherent loss, the histograms of both original and decrypted images were compared and shown in Figure 2 (Baboon), Figure 3 (Lena), and Figure 4 (Eggs). The pixel histogram test revealed that the distribution of the plain images and their decrypted image counterparts have the same pixel histogram distributions, which means that there is a high correlation between the original images and decrypted images. Hence, the proposed scheme can fully recover the original image without any noticeable loss of features.

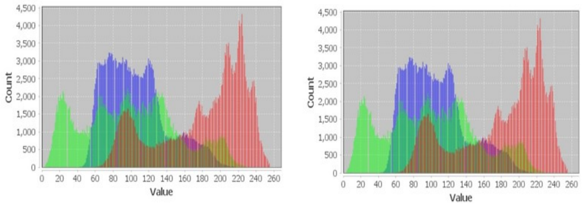
B. Encoding Analysis

The encoding analysis generated some results, as presented in Tables 1 and 2. Table 1 shows that the size of the images reduced meaningfully. This pronounced reduction in size means that there will be a very fast transmission rate of the encrypted images during transmission since very few bits will now be used to represent the encrypted images while being transmitted. Also, since the size has reduced, it means the memory requirement for storing the encrypted images is also reduced and has been presented in Table 2. Also, from the results presented in Table 2, the developed system achieved in terms of encryption and decryption time when compared with the results presented by [4]-[6].



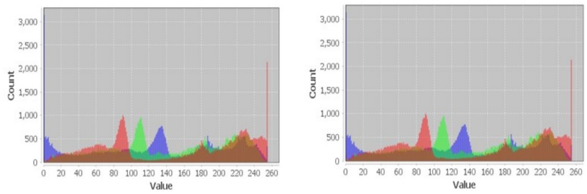
(a) Original (b) Decrypted

Figure 2. Histograms of original and decrypted Baboon image



(a) Original (b) Decrypted

Figure 3. Histograms of original and decrypted Lena image



(a) Original (b) Decrypted

Figure 4. Histograms of original and decrypted Eggs image

C. Security Analysis

The security and strength of the encryption system are analyzed by subjecting outputs from the system to histogram analysis. Encrypted images are always well secured against statistical attack when its histogram encrypts information about the encrypted image and also totally different from the histogram information of the unencrypted image [5], [6]. Figure 5(a) shows the histograms of the unencrypted and encrypted images of baboon.png, while Figure 5(b) presents the histograms for egg.png. It can be deduced that the encrypted and unencrypted histograms do not have any statistical similarities. Hence, the system can be perceived to be highly secured. Other techniques that can be used in this regard include the correlation coefficient analysis, key space analysis, or key sensitivity analysis.

However, from the results presented, it has been revealed that owing to the reduced size as a result of the gray code arithmetic values, encrypted images require a few numbers of bits to represent each pixel. The

Table 1. Sizes of unencrypted, encrypted and decrypted images compared

Image name & format	Pixel size	Initial size (kb)	Size on disk		
			Encrypted size (kb)	Compression ratio (%)	File size after decryption
Baboon (png)	512 * 512	622	304 kb	51.1	625 kb
Lena (png)	512 * 512	500	217 kb	56.6	503 kb
Eggs (jpg)	300 * 250	13.2	5 kb	62.1	13.3 kb

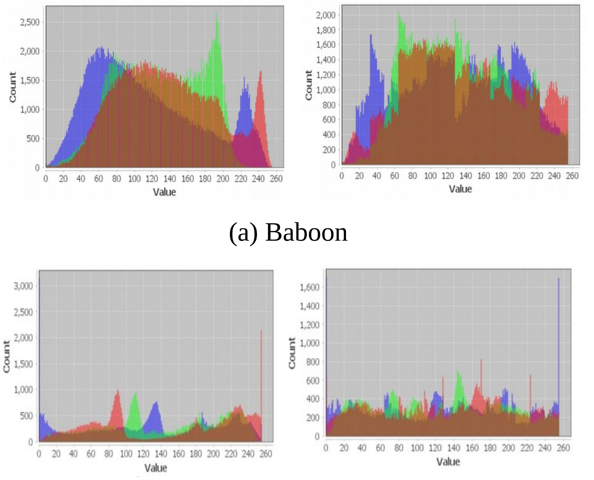
Table 2. Memory requirement of unencrypted, encrypted and decrypted images compared

Image name & format	Number of elements	Encryption time (Secs)	Decryption time (Secs)	Memory requirement (Bytes)		
				Unencrypted	Encrypted	Decrypted
Baboon (png)	262,144	7	7	636,928	311,296	640,000
Lena (png)	262,144	5	6	512,000	222,208	515,072
Eggs (jpg)	75,000	3	3	13,516.8	5,120	13,619.2

proposed scheme is resistant to statistical attacks, which makes it highly secured. The scheme outperforms the schemes in [4]-[6], [38] in terms of computational time, and its ability to secure non-square images. The developed scheme could be used for protecting privacy in biometrics, medical imaging systems, and video surveillance systems. In the challenges for the future, the researcher intends to perform other listed statistical analyses and also extend the scheme to test its applicability in securing continuous images (video).

IV. Conclusion

This scheme presented an image cryptosystem that encrypted various digital image types and sizes, reduction in computational complexity in encryption and decryption processes of digital images and an improved efficiency in terms of the processes involved in securing a digital image by developing a position-based pixel value transformation algorithm. This research work has introduced a value transformation-based cryptosystem that selects algorithm for pixel transformation based on its position and offers better encryption without the need for pixel scrambling.



(a) Baboon

(b) Eggs

Figure 4. Histograms of unencrypted and encrypted images

References

[1] A. N. Babatunde, “Methodology for Image Cryptosystem Based on Gray Code Number System,” *Computing and Information Systems Journal*, vol. 23, no. 2, pp. 1-10, 2019.

[2] S. Alhassan, “Enhancement of security of digital image using the moduli sets,” *thesis*, University of Development Studies, Ghana, 2013.

[3] O. Oshodi, “Gray code number system based digital image cryptosystem,” *thesis*, College of Information and Communication Technology, Kwara State University, Nigeria, 2018.

[4] P. D. Oyinloye and K. A. Gbolagade, “An improved image scrambling algorithm using {2n -1, 2n, 2n +1},” *Computing and Information Systems Journal*, vol. 22, no. 3, pp. 1-7, 2018.

[5] S. Alhassan and K. A. Gbolagade, “Enhancement of security of digital image using the moduli set (2n-1, 2n, 2n-1),” *International Journal of Advanced Research in Computer Engineering and Technology*, vol. 2, no. 7, pp. 2223-2229, 2013.

[6] S. Alhassan, “Enhancement of security of digital image using the moduli sets,” *thesis*, University of Development Studies, Ghana, 2013.

[7] H. Darshana and S. Parinder, “A comprehensive survey of video encryption algorithms,” *International Journal of Computer Applications*, vol. 59, no. 1, pp. 14-19, 2012. doi: 10.5120/9512-3902

[8] W. Puech, Z. Erkin, M. Barni, S. Rane, and R. L. Lagendijk, “Emerging cryptographic challenges in image and video processing,” in *19th IEEE International Conference on Image Processing*, Orlando, USA, Oct. 2012, pp. 2629-2632. doi: 10.1109/ICIP.2012.6467438

[9] V. Potdar and E. Chang, ”Disguising text cryptography using image cryptography,” in *4th*

International Network Conference, Plymouth, UK, Jul. 2004.

[10] A. N. Babatunde, R. G. Jimoh, and K. A. Gbolagade, "An algorithm for a residue number system based video encryption system," *Computer Science Series Journal*, vol. 14, no. 2, pp. 136-147, 2016.

[11] A. Abdul-Barik, "Enhancement of the security and compression of the Lempel-Ziv-Welch's algorithm using residue number system for efficient transmission via network communication channels," *thesis*, University of Development Studies, Ghana, 2016.

[12] Y. Zhou, K. Panetta, S. Agaian, and P. C. Chen, "(n, k, p)-Gray Code for Image Systems," *IEEE Transactions on Cybernetics*, vol. 42, no. 2, pp. 515-529, 2013. doi: 10.1109/TSMCB.2012.2210706

[13] A. Ahmad and F. Bait-Shiginah, "A nonconventional approach to generating efficient binary gray code sequences," *IEEE Potentials*, vol. 31, no. 3, pp. 16-19, 2012. doi: 10.1109/MPOT.2011.2178193

[14] I. Nasir, W. Ying, and J. Jianmin, "A new robust watermarking scheme for color image in spatial domain," in *3rd International IEEE Conference Signal-Image Technologies and Internet-Based System*, Shanghai, China, Dec. 2007, pp. 942–947. doi: 10.1109/SITIS.2007.67

[15] H. W. Tseng and C. C. Chang, "Anti-pseudo-gray coding for VQ encoded images over noisy channels," *IEEE Communication Letters*, vol. 11, no. 5, pp. 443-445, 2007. doi: 10.1109/LCOMM.2007.070074

[16] W. S. Chen, K. H. Chih, S. W. Shih, and C. M. Hsieh, "Personal identification technique based on human IRIS recognition with wavelet transform," in *IEEE International Conference on Acoustics, Speech, and Signal Processing*, Philadelphia, USA, Mar. 2005, pp. 949-952. doi: 10.1109/ICASSP.2005.1415563

[17] S. Erturk, "Locally refined Gray-coded bit-plane matching for block motion estimation," in *3rd International Symposium on Image and Signal Processing and Analysis*, Rome, Italy, Sept. 2003, pp. 128–133. doi: 10.1109/ISPA.2003.1296881

[18] W. Ding, W. Yan, and D. Qi, "Digital image scrambling," *Progress in Natural Science*, vol. 11, no. 6, pp. 454-460, 2001.

[19] S. J. Ko, S. H. Lee, S. W. Jeon, and E. S. Kang, "Fast digital image stabilizer based on Gray-coded bit-plane matching," *IEEE Transactions on Consumer Electronics*, vol. 45, no. 3, pp. 598–603, 1999. doi: 10.1109/30.793546

[20] J. Ludman, "Gray code generation for MPSK signals," *IEEE Transmission Communication*, vol. 29, no. 10, pp. 1519–1522, 1981. doi: 10.1109/TCOM.19https://doi.org/81.1094886

[21] M. B. Younes and J. Aman, "An image encryption approach using a combination of permutation technique followed by encryption," *International Journal of Computer Science and Network Security*, vol. 8, no. 4, pp. 191-197, 2008.

[22] T. Gao and Z. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, Solitons & Fractals*, vol. 38, no. 1, pp. 213-220, 2008. doi: 10.1016/j.chaos.2006.11.009

[23] Y. Shen, G. Zhang, X. Li, and Q. Liu, "An improved image encryption method based on total shuffling scheme," in Advances in Computer Science and Information Engineering, Springer-Verlag, 2012, pp. 643-650.

[24] R. -G. Zhou, Y. J. Sun, and P. Fan, "Quantum image Gray-code and bit-plane scrambling," *Quantum Information Processing*, vol. 14, pp. 1717-1734, 2015.

[25] T. Sivakumar and R. Venkatesan, "A new image encryption method based on knight's travel path and true random number," *Journal of Information Science and Engineering*, vol. 32, pp. 133-152, 2016.

[26] N. K. Pareek, "Knight's tour application in digital image encryption," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, no. 9, pp. 208-213, 2015.

[27] K. Gupta, R. Gupta, R. Agrawal, and S. Khan, "An ethical approach of block based image encryption using chaotic map," *International Journal of Security and Its Applications*, vol. 9, no. 9, pp. 105-122, 2015. doi: 10.14257/ijsia.2015.9.9.10

[28] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926-934, 2006. doi: 10.1016/j.imavis.2006.02.021

[29] H. T. Panduranga and S. K. Naveen, "A novel image encryption approach using B2g And G2b code conversion technique," *International Journal on Computer Engineering and Information Technology*, vol. 1, no. 1, 2009.

[30] K. Brindha, R. Sharma, and S/ Saini, "Use of symmetric algorithm for image encryption," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 5, pp. 4401- 4407, 2014.

[31] A.B.Y. Mohammad, and J. Aman, "Image encryption using block-based transformation algorithm," *IAENG International Journal of Computer Science*, vol. 35, no. 1, 2008.

[32] A. Musheer and A.M. Shamsher, "A new algorithm of encryption and decryption of images using chaotic mapping," *International Journal on Computer Science and Engineering*, vol. 2, no. 1, pp. 46-50, 2009.

[33] A. S. Rathore, K. Patidar, and G. S. Chandel, "A review on recent trends in image encryption techniques," *International Journal of Engineering Technology and Applied Science*, vol. 2, no. 5, 2016.

[34] W. Auyporn, and S. Vongpradhip, "A robust image encryption method based on bit plane decomposition and multiple chaotic maps," *International Journal of Signal Processing System*, vol. 3, no. 1, pp. 8-13, 2015.

[35] A. Nag et al., "Image encryption using affine transform and xor operation," in *International Conference on Signal Processing, Communication, Computing and Networking Technologies*, Thuckafay, India, Jul. 2011, pp. 309-312. doi: 10.1109/ICSCCN.2011.6024565

[36] A. Goel and N. Chandra, "A technique for image encryption with combination of pixel rearrangement scheme based on sorting group-wise of RGB values and explosive inter-pixel displacement," *International Journal of Image, Graphics and Signal Processing*, vol. 4, no. 2, pp. 16-22, 2012. doi: 10.5815/ijigsp.2012.02.03

[37] P. K. Naskar and A. Chaudhuri, "A secure symmetric image encryption based on bit-wise operation," *International Journal of Image, Graphics and Signal Processing*, vol. 6, no. 2, pp. 30-38, 2014. doi: 10.5815/ijigsp.2014.02.04

[38] P. S. Ghode, P. P. Patil, V. Nayyar, and S. Moghe, "A keyless approach to lossless image encryption," *International Journal of Advanced Research in Science*, vol. 4, no. 5, pp. 1459- 1467, 2014.

[39] R. Liu, "New binary image encryption algorithm based on combination of confusion and diffusion," *Journal of Chemical and Pharmaceutical Research*, vol. 6, no. 7, pp. 621-629, 2014.

[40] A. Singh and N. Dhanda, "DIP using image encryption and xor operation affine transform," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 17, no. 2, pp. 07-15, 2015.

[41] A. Mitra, Y.V.R. Subba and S.R.M Prasanna, "A new image encryption approach using combinational permutation techniques," *International Journal of Electrical and Computer Engineering*, vol. 1, no. 2, pp. 127-131, 2006.

[42] B. A. Weyori, P. N. Amponsah, and P.K. Yeboah, "Modeling a secured digital image encryption scheme using a three moduli set," *Global Journal of Computer Science and Technology Interdisciplinary*, vol. 12, no. 10, 2012.

[43] D. Chattopadhyay, M.K. Mandal and D. Nandi, "Symmetric key chaotic image encryption using circle map," *Indian Journal of Science and Technology*, vol. 4, no. 5, pp. 593-599, 2011.

[44] K. Struss, "A chaotic image encryption," in *Mathematics Senior Seminar*, University Minnesota, USA, 2009, pp. 1-19.

[45] K. -L. Chung and L. -C. Chang, "Large encrypting binary images with higher security," *Pattern Recognition Letters*, vol. 19, no. 43, section 4, pp. 461-468, 1998. doi: 10.1016/S0167-8655(98)00017-8

[46] S. Li-Ping, Q. G. Zheng, H. Hong-Jiang, and H. Xing-Chen, "2D triangular mappings and their applications in scrambling rectangle image," *Information Technology Journal*, vol. 7, no. 1, pp. 40-47, 2008. doi: 10.3923/itj.2008.40.47

[47] Z. Linhua, L. Xiaofeng, and W. Xuebing, "An image encryption approach based on chaotic maps," *Chaos, Solitons and Fractals*, vol. 24, no. 3, pp. 759–765, 2005. doi: 10.1016/j.chaos.2004.09.035

[48] M. Salleh, S. Ibrahim, and I. F. Isnin, "Image encryption algorithm based on chaotic mapping," *Jurnal Teknologi*, vol. 39, no. 1, pp. 1-12, 2003. doi: 10.11113/jt.v39.458

[49] M. Mishra, P. Mishra, M.C. Adhikary, and S. Kumar, "Image encryption using fibonacci-lucas transformation," *International Journal on Cryptography and Information Security (IJCIS)*, vol.2, no. 3, pp. 131-141, 2012.

[50] S. S. Yadav, Y. Singh, and S. K. Sriwas, "Gray code (n, k, p) based pixel substitution and affine transform based gray code bit plane permutation technique for secure image encryption," *ARPN Journal of Engineering and Applied Sciences*, vol. 12, no. 11, pp. 3500-3508, 2017.

[51] S. S. Yadav, Y. Singh, and S. K. Sriwas, "Hybrid image encryption technique to improve the security level by using (n, k, p) gray code and xor operation," *Indian Journal of Science and Technology*, vol. 10, no. 20, pp. 1-9, 2017. doi: 10.17485/ijst/2017/v10i20/113180

[52] S. Al-Maadeed, A. Al-Ali, and T. Addalla, "A new chaos-based image-encrytion and compression algorithm," *Journal of Electrical and Computer Engineering*, vol. 2012, pp. 1-11, 2012. doi: 10.1155/2012/179693

[53] J. Yang, "Algorithm of image information hiding based on new anti-arnold tranform and blending in DCT," in *IEEE 12th International Conference on Communication Technology*, Nanjing, China, Nov. 2010, pp. 312-315. doi: 10.1109/ICCT.2010.5689227