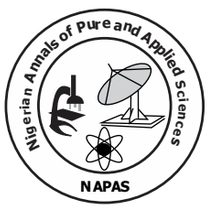


-

Evaluation of Aizawa Chaotic Map in Digital Image Protection

Gbaden Terlumun
Mathematics/Statistics/Computer Science
University of Agriculture, Makurdi Benue State
gbaden2014@gmail.com. 07037381034.

Abstract

In recent years, great concerns have been raised regarding the issue of digital image protection due to the increasing demand for security services. To meet this challenge, a novel chaos-based approach is suggested in this paper. To address the security and efficiency problems encountered by many existing permutation-diffusion type image ciphers the new scheme utilizes Aizawa chaotic map which enhances the security against known/chosen –plaintext attack. Experimental tests were carried out and the results indicate that the proposed scheme provides an effective and efficient way for real-time secure digital image transmission over unsecured networks.

Introduction

The rapid development of the internet has created an environment to disclose confidential information to illegal users, such as personal image. Transmissions of multimedia files across the world over public networks in all fields of the society are on the increase. However, those networks are not secured for the direct transmission of private messages. The different types of files such as text, image and video have to face the threat of unsafety. In order to maintain secrecy and to make use of the networks already developed simultaneously, the study of image encryption has become an important aspect of protecting security of image information (Yakubu and Aboiyar, 2017). Hence, covert communication methods aroused the interest of many researchers and are becoming the world's attentive focus. Traditional encryption methods such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES) are not suitable for image encryption since digital image possesses some inherent features such as bulk data capacity and high correlation among adjacent pixels, the image size is almost always much greater than that of text and it needs much time to directly encrypt the image data using software implementation of traditional cryptosystems. Properties of chaos, such as randomness, ergodicity, sensitivity to initial conditions and control parameters have proved to be suitable for designing the means for data protection, especially image encryption. During the past decade, many chaos-based cryptographic techniques have been studied, such as the chaos-based secret communication, chaos-based block/stream cipher, chaos-based random number generation (Biswas, 2013). Additionally, some applications based on chaos have been investigated. For example, chaos-based image encryption or authentication, video/audio scrambling, multimedia and copyright protection chaos-based cryptography is a new research field across two fields, i.e chaos (nonlinear dynamic system) and cryptography (computer and data security) (Baker and Gollub, 1990). Chaotic maps are very suitable for constructing encryption algorithms. In addition, chaotic ciphers are generally easy to implement and have fast speed, low resource consumption, which shows a clear advantage for multimedia data encryption. Therefore, chaotic maps provide a good application for the secure transmission of multimedia data encryption (Auyporn and Vongpradhp, 2015).

In this work, an image encryption algorithm based on Aizawa chaotic map is addressed, with the goal of providing an efficient and secure way for image encryption.

Chaos-Based Image Encryption

Zhe *et al.* (2010) affirmed to the fact that in recent years, there is a growing of research interest of chaos and cryptography. With the desirable properties of ergodicity and high sensitivity to the initial condition and parameters, chaotic maps are very suitable for constructing encryption algorithms. In addition, chaotic ciphers are generally easy to implement and has fast speed, low resource consumption, which show a clear advantage for multimedia data encryption. They concluded that chaotic maps provide a good application for the secure transmission of multimedia data encryption. Radha and Venkatesulu (2012) introduced a block cipher algorithm, which encrypted and decrypted a block size of 512 bits regardless of the file format. In this, a permutation algorithm using a chaotic system was employed to provide the shuffler function. A shuffler operator was defined using the shuffler function. A random key generator generated key sequences and the scheme employed key-dependent transformations based on distance in the shuffling operator. The process of encryption/decryption was governed by the shuffler function, shuffler operator and the pseudorandom key. This was to solve the problem of widespread use of image, audio and video data which makes media content protection increasingly necessary and important. They proposed a naive approach which treated the multimedia signal to be protected as a text and use proposed encryption design to encrypt the whole data stream. Upon reception, the entire cipher text data stream would be decrypted and playback can be performed at the client end with an initial time delay. The basic operation used was logical XOR and so the algorithm had a very high encryption/decryption speed. The execution time proved that the proposed scheme was faster than the existing cryptographic schemes. The proposal of the algorithm was to manage the tradeoffs between the speed and security and hence

appropriate for real-time image and video communication applications. Pande and Zambreno (2011) stated that chaotic encryption schemes are believed to provide greater level of security than conventional ciphers. In their research, a chaotic stream cipher was first constructed and then its hardware implementation details over Xilinx Virtex-6 FPGA were provided. Logistic map was the simplest chaotic system and had high potential to be used to design a stream cipher for real-time embedded systems. Its simple construct and non-linear dynamics made it a common choice for such applications. They presented a modified logistic map which improved the performance of logistic map in terms of higher Lyapunov exponent and uniformity of bifurcation map. It also avoided the stable orbits of logistic map giving a more chaotic behavior to the system. A stream cipher was built using modified logistic map and random feedback scheme. The proposed cipher gave 16 bits of encrypted data per clock cycle. The hardware implementation results over Xilinx Virtex-6 FPGA gave a synthesis clock frequency of 93 MHz and a throughput of 1.5 Gbps while using 16 hardware multipliers. This made the cipher suitable for embedded devices which tight constraints on power consumption, hardware resources and real-time parameters. In their work, Al-Maadeed *et al.* (2012) proposed a new and efficient method to develop secure image-encryption techniques. The new algorithm combines two techniques encryption and compression. In this technique, a wavelet transform was used to decompose the image and decorrelate its pixels into approximation and detail components. The more important component (the approximation component) was encrypted using a chaos-based encryption algorithm. This algorithm produces a cipher of the test image that had good diffusion and confusion properties. The remaining components (the detail components) were compressed using a wavelet transform. This proposed algorithm was verified to provide a high security level. A complete specification for the new algorithm was provided. Several text images were used to demonstrate the validity of the proposed algorithm. The results of several experiments show that the proposed algorithm for image cryptosystems provided an efficient and secured approach to real-time image encryption and transmission. Sankaran and Krishna (2011) revealed that recent researches of image encryption algorithms have been increasingly based on chaotic systems, but the drawbacks of small key space and weak security in one dimensional chaotic cryptosystems are obvious. The research considered a new image encryption scheme which employs one of the three dynamic chaotic systems (Lorenz or Chen or Lu chaotic system selected based on 16-byte key) to shuffle the position of the image pixels (pixel position permutation) and uses another one of the same three chaotic maps to confuse the relationship between the cipher image and the plain image (pixel value diffusion), thereby significantly increasing the resistance to attacks. The proposed system had the advantage of bigger key space, smaller iteration times and high security analysis such as key space analysis, statistical analysis and sensitivity analysis which were carried out. The results demonstrated that the proposed system was highly efficient and robust. According to Xiao-Jun *et al.* (2012) the wireless sensor network (WSN) has been widely used in various fields, but it still remains in the preliminary discovery and research phase with a lack of various related mature technologies. Traditional encryption schemes are not suitable for wireless sensor networks due to intrinsic features of the nodes such as low energy, limited computation capability, and lack of storage resources (Zhang and Dong, 2010). The research presented a novel block encryption scheme based on the integer discretization of a chaotic map, the Fiestel network structure and an S-block. The novel scheme was fast, secure, has low resource consumption and was suitable for wireless sensor network node encryption schemes. The experimental tests were carried out with detailed analysis, showing that the novel block algorithm has a large key space, very good diffusion and disruptive performances, a strict avalanche effect, excellent statistical balance and fast encryption speed. These features enable the encryption schemes to pass the SP800-22 test. Meanwhile the analysis and the testing of fields, time and storage space on the simulator platform show that this new encryption scheme is well able to hide information in the wireless sensor. Wang *et al.* (2015) proposed a new block image encryption scheme based on hybrid chaotic maps and dynamic random growth technique. Since cat

map is periodic and can be easily cracked by chosen plaintext attack, they used cat map in another securer way which can completely eliminate the cyclical phenomenon and resist chosen plaintext attack. In the diffusion process, an intermediate parameter is calculated according to the image block. The intermediate parameter is used as the initial parameter of chaotic map to generate random data stream. In this way, the generated key streams are dependent on the plaintext image, which can resist the chosen plaintext attack. The experimental results proved that the proposed encryption algorithm is secured enough to be used in image transmission systems. Telem *et al.* (2014) introduced a robust gray image encryption scheme using chaotic logistic map and artificial neural network (ANN). In the proposed method, an external secret key was used to derive the initial conditions for the logistic chaotic maps which were employed to generate weights and biases matrices of the multilayer perception (MLP). During the learning process with back propagation algorithm, ANN determines the weight matrix of the connections. The plain image was divided into four subimages which were used for the first diffusion stage. The sub images obtained previously were divided into the square sub image blocks. In the next stage, different initial conditions were employed to generate a key stream which was to be used for permutation and diffusion of the sub image blocks. Some security analyses such as entropy analysis, statistical analysis, and key sensitivity analysis were given to demonstrate the key space of the proposed algorithm which was large enough to make brute force attacks infeasible. Computing validation using experimental data with several gray images has been carried out with detailed numerical analysis, in order to validate the high security of the proposed encryption scheme. Misra *et al.* (2011) considered chaotic encryption as a way of cryptography. The chaotic encryption algorithms have several advantages over the traditional encryption algorithms like high security, speed, reasonable computational overheads and computational power (Zang and He, 2001). These algorithms use the chaotic system properties like loss of information and are sensitive to initial condition. Several chaos based encryption methods have been proposed and discussed in the last one decade. To obtain higher performance, these methods take benefit of the more and more complex behavior of chaotic signals. This work is a contribution by comparing and analyzing the performance of the previous chaotic image encryption methods. Liu *et al.* (2014) designed a chaos-based color image encryption scheme using bijection. The whole image was diffused by exclusive or (XOR) operation for random rounds, each color component was separated into blocks with the same size. A bijective function f:B S between block set B and S box set S was built. The corresponding 8 x 8 S box was dynamically generated by the Chen system with variable conditions. The ciphered image can be obtained after substituting each block with the paired S box. Numerical simulation and security analysis demonstrated that the scheme was practical in image encryption. Mankar and Mishra (2011) proposed three different chaotic encryption methods using 1-D chaotic map known as Logistic map named as Logistic, NLFSR and modified NLFSR according to the name of chaotic map and non-linear function involved in the scheme. The designed schemes have been crypt analyzed for five different methods for testing its strength. Cryptanalysis has been performed for various texts using various keys selected from domain of key space. Logistic and NLFSR methods were found to resist known plaintext attack for available first two characters of plaintext. Plaintext sensitivity of both methods was within small range along with medium key sensitivity. Identifiability for keys of first two of the scheme has not been derived concluding that methods may prove to be weak against brute-force attack. In the last modified scheme avalanche effect found to be improved compared to the previous ones and method was found to resist brute-force attack as it derives the conclusion for identifiability. Guanghui *et al.* (2014) stated that in the field of chaotic image encryption, the algorithm based on correlating key with plain text has become a new developing direction. However, for this kind of algorithm, some shortcomings in resistance to reconstruction attack, efficient utilization of chaotic resource, and reducing dynamical degradation of digital chaos were found. In order to solve these problems and further enhance the security of encryption algorithm, based on disturbance and feedback mechanism, we present a new image encryption scheme. In the running-key generation

stage, by successively disturbing chaotic stream with cipher-text, the relation of running-key to plaintext was established, reconstruction attack was avoided, effective use of chaotic resource was guaranteed, and dynamical degradation of digital chaos was minimized. In the image encryption stage, by introducing random-feedback mechanism, the difficulty of breaking this scheme was increased. Comparing with the state-of-the-art algorithm, our scheme exhibits good properties such as large key space, long key period, and extreme sensitivity to the initial key and plaintext. Therefore, it can resist brute-force, reconstruction attack and differential attack. Intelligent transportation systems (ITS) are advanced applications in which the transportation industry is adapted to the information technology revolution. As an important development direction of ITS, the electronic toll collection (ETC) subsystem, which enables an efficient and speedy toll collection has gained widespread popularity in the world (Tang *et al.,* 2014). In an ETC system, toll transaction data are transmitted over intelligent transportation network, which is vulnerable to eavesdropping, interfering and tampering attacks. To address the above security problems, the researchers proposed a chaotic stream cipher-based cryptographic scheme to realize secure data communication over wireless sensor network (WSN), which is a part of ITS. The proposed cryptographic scheme allowed ITS to achieve key negotiation and data encryption between sensor nodes in the WSN, while as reduced computational costs and power consumption security analysis and experimental results showed that the proposed scheme could protect the transmission between wireless sensor nodes from being attacked, and significantly reduced the communication overhead for the whole system compared to the existing ECC-AES scheme, thus satisfying the real-time data transmission requirement of ITS(Zhang *et al.*, 2015). A novel video encryption scheme based on multiple digital chaotic systems was proposed by Li *et al.* (2015). They called it Chaotic Video Encryption Scheme (CVES). CVES is independent of any video compression algorithms, and can provide high security for real-time digital video with fast encryption speed, and can be simply realized both by hardware and software. Moreover, CVES can be extended to support random retrieval of cipher-video with considerable maximal time-out; the extended CVES is called RRS-CVES (Random-Retrieval-Supported CVES). Essentially speaking, CVES is a universal fast encryption system and can be easily extended to other real-time applications. In CVES, 2^n chaotic maps are used to generate pseudo-random signal to mask the video, and to make pseudo-random permutation of the masked video. Another single chaotic map is employed to initialize and control the above 2^n chaotic maps. Discussions were presented to estimate the performance of CVES/RRS-CVES respectively from the viewpoints of speed, security, realization and experiments. In this research Jastrzebski and Kotulski (2009) examined one of the recently proposed chaotic image encryption algorithms, based on chaotic map lattices (CML). They show certain problems with the chaotic map, as well as errors in the designed algorithm. Then the researchers proposed a way to improve on it and presented a new version of the algorithm and its implementation. Comparison of both schemes as well as security analysis formed the result of the research. In present times, due to the rapidly growth of digital and multimedia applications, more multimedia data were developed and transmitted through the network in art, entertainment, advertisement, education, training and commercial areas, which may have important information that should not be accessed by general users. Therefore, the issue of protecting the confidentiality, integrity, security, privacy as well as the authenticity of images has become an important issue for communication and storage of images. In recent years, various encryption techniques were developed and applied to protect the confidential images from unauthorized users. Kumaur *et al.* (2015) presented a review on different chaotic based image encryption and existing different image encryption techniques based on chaos to design an image cryptosystem. In their work, they first presented a general introduction for cryptography and image encryption and followed by discussion of different chaotic based image encryption techniques and related works for each technique reviewed. Finally, the main purpose of their paper, to help in the design of a new chaotic based image encryption technique in future by studying the behavior of several existing chaotic based image encryption algorithms. For high-security, encryption is one of the ways to protect the

information from leakage. Many applications like military image database, medical imaging system and online personal photograph album require fast and robust security system because they are stored and transferred through network. Image encryption is the conversion of image to a distorted form so that it can be secured from unauthorized users. In their research, Kaur and Gupta (2016) reviewed some image encryption techniques and finally investigated two methods for image encryption. First technique was encryption of image by linear congruential generator. Random numbers were generated by prime modulo multiplicative linear congruential generator. These numbers were used as index for shuffling of rows, columns and pixels of an image. Second technique uses logistic maps to generate random number sequence. These random numbers were used as index for shuffling of rows, columns and pixels of an image. Finally, the authors analyzed two methods on the basis of image quality parameters.

Proposed System

In this section, Aizawa Chaotic Encryption Method which seems to be much better than traditional encryption methods is proposed. These are the three dimensional chaotic encryption scheme using the Aizawa system. Chaotic encryption is the new direction of cryptography. It makes use of chaotic system properties such as sensitivity to initial conditions and parameters, ergodicity and lot of information. Cryptographic designs are synthesized based on cryptographic primitives including Aizawa chaotic map.

The Aizawa system

The Aizawa attractor is a system of equations that, when applied iteratively on three-dimensional coordinates, evolves in such a way as to have the resulting coordinates map out a three dimensional shape, in this case a sphere with a tube-like structure penetrating one of its axis. The equations themselves are fairly straightforward:

$$\begin{aligned} dx &= (z-b)x - dy \\ dy &= dx + (z-b)y \\ dz &= c + az - \frac{z^3}{3} - x^2 + fzx^3 \end{aligned} \qquad (1)$$

where a = 0.95, b = 0.7, c = 0.6, d = 3.5, e = 0.25, f = 0.1. Each previous coordinate is input into the equations, the resulting value multiplied by a time value (here arbitrarily chosen as 0.1) and then added to the previous value.

When coded, the attractor evolves into a beautiful sphere with a tube-like structure penetrating down its y- axis.

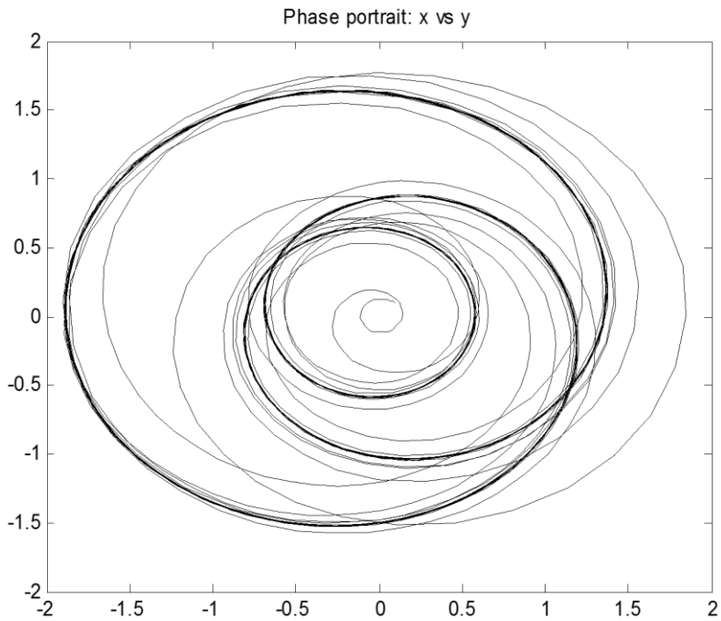


Figure 1: Phase portrait of Aizawa attractor

Algorithm of the Proposed System

In this section, we present the detail algorithm for encryption/decryption of coloured images using Aizawa chaotic map.

(i) **Input**: RGB, M,N, a, b, c, d, e, f, h, x_0, y_0, z_0

(ii) **Output**: Encrypted plain image using x_m, y_m, z_m

(iii) Read RGB image I

(iv) Obtain the image size M x N = N (N is the size of image per colour)

(v) Enter the parameters a, b, c, d, e, f, h(step size), x_0, y_0, z_0(initial values)

(vi) Solve the Aizawa system for N time steps using Runge-Kutta method to get x,y,z (as explained in subsection 3.3.4)

(vii) Preprocess by getting rid of the integral part of real numbers, so that the value of the domains of x,y,z becomes a real unified sequence value.

$$x(i) = 10^n x(i) - round\left(10^n x(i)\right)$$
$$y(i) = 10^n y(i) - round\left(10^n y(i)\right)$$
$$z(i) = 10^n z(i) - round\left(10^n z(i)\right)$$

(viii) Sort x,y,z to obtain xyz with their test of indices l_x, l_y and l_z (as explained in subsection 3.3.3)

(ix) Define R, G and B as matrices for red, green and blue.

(x) Reshape R, G and B into row matrices and scramble them using the solution of the Aizawa system to give R, G and B (confusion).

(xi) Use XOR operations for diffusion to obtain R′, G′ and B′.

(xii) Reshape R′, G′ and B′ into M x N matrices to obtain $\widetilde{R}, \widetilde{G}$ and $\tilde{B}$

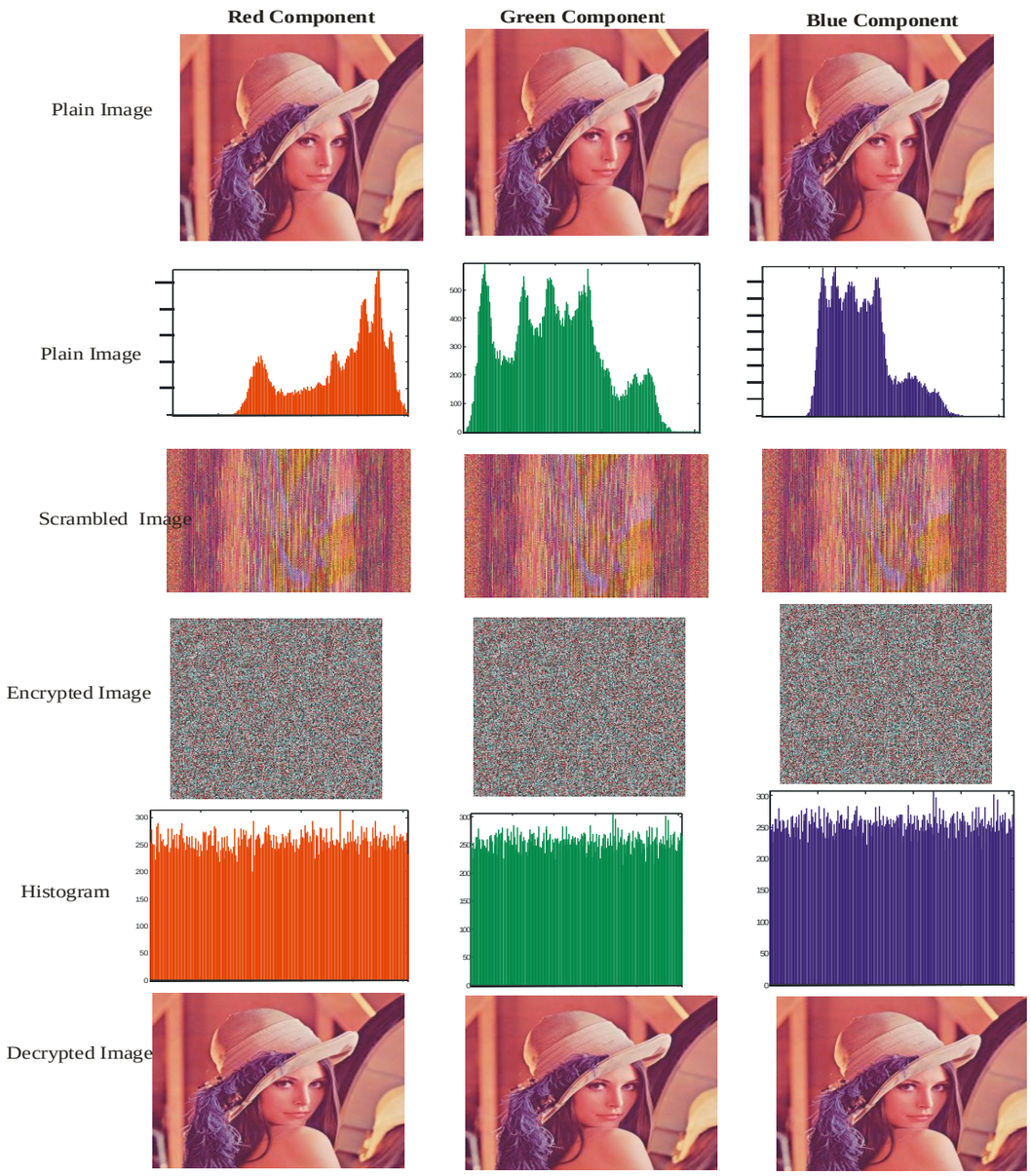
(xiii) Form encrypted image

Reverse steps can be used for decryption.

Experimental Results

We conducted this experiment using Hp 250 G5 computer with a processing speed of 1.6GHZ and a RAM size of 2048MB. Two RGB images mandril_color_256.tif and Lena_color_256.tif were used in testing the digital image encryption algorithm using the Aizawa chaotic map. The source of these input data is from USC-SIPI (University of Southern California-Signal and Image Processing Institute) database.

Below are the results of the simulations of the digital image encryption algorithm using Aizawa chaotic map.


Red Component
Green Component
Blue Component
Plain Image
Plain Image
Scrambled Image
Encrypted Image
Histogram
Decrypted Image

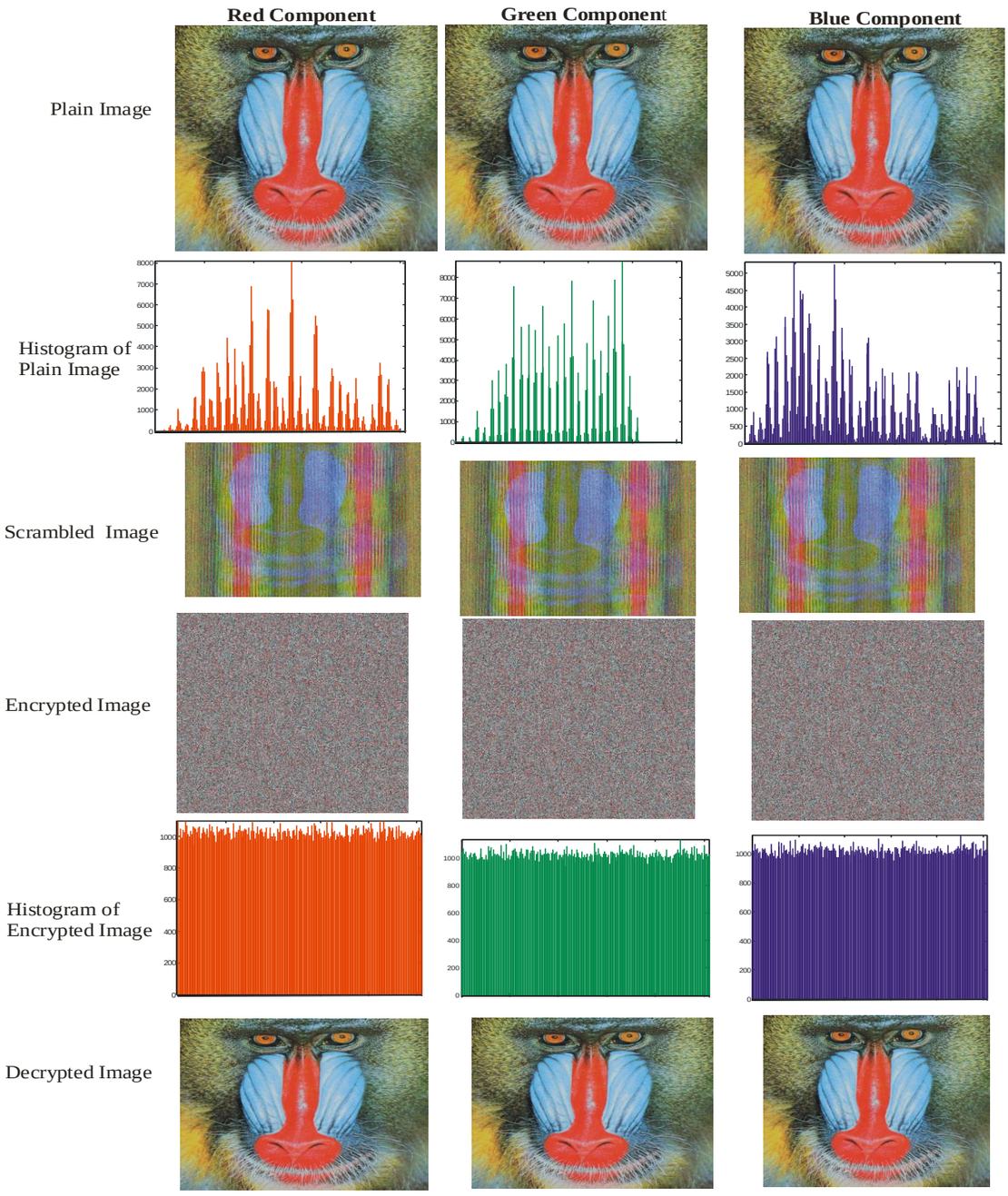


Figure 3: Histogram of Plain, Scrambled and Encrypted colour image of mandril using Aizawa chaotic image encryption scheme.

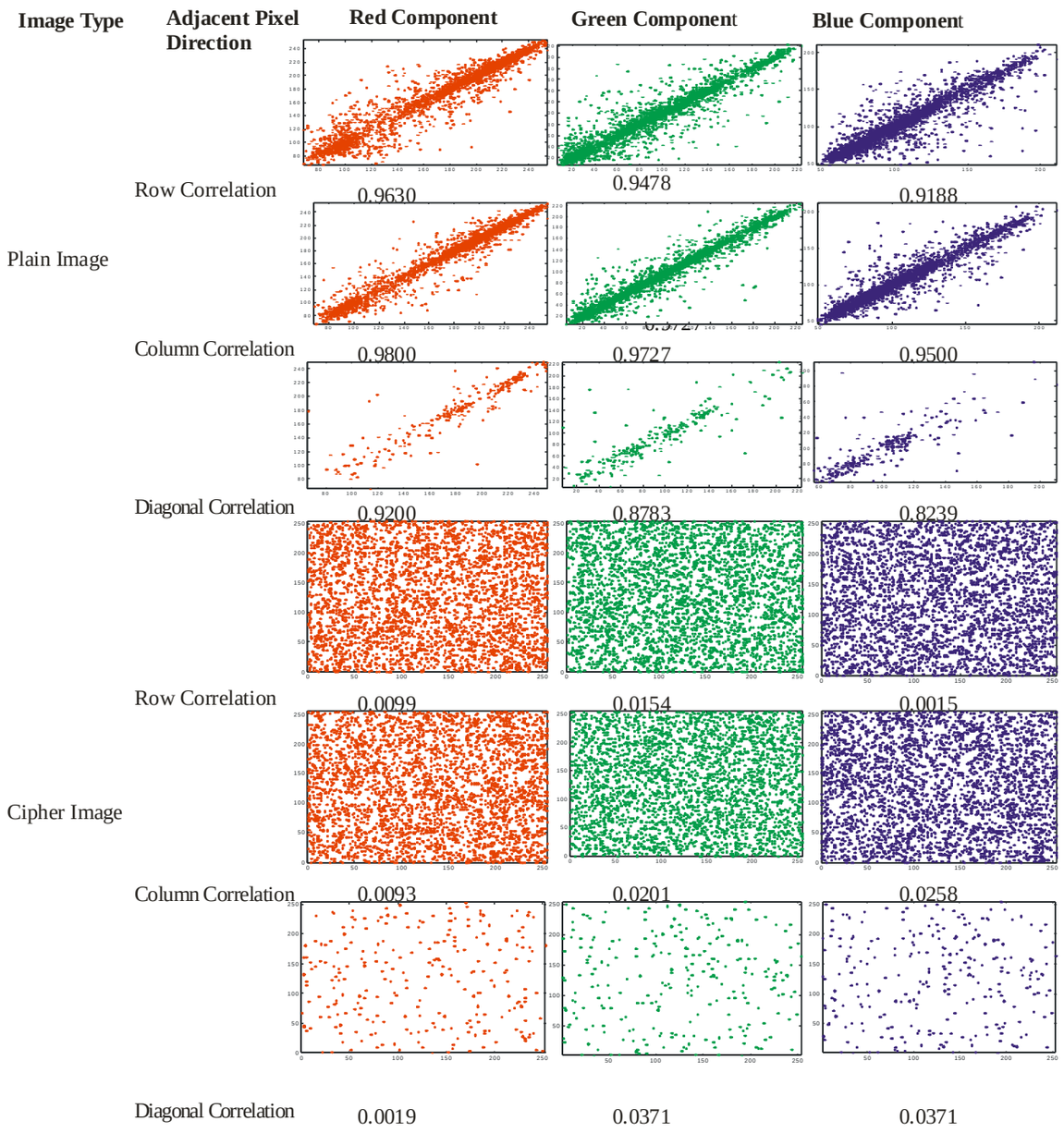


Figure 4: Correlation between adjacent pixels of the plain and the cipher colour image of Lena using the **Aizawa** chaotic image encryption algorithm.

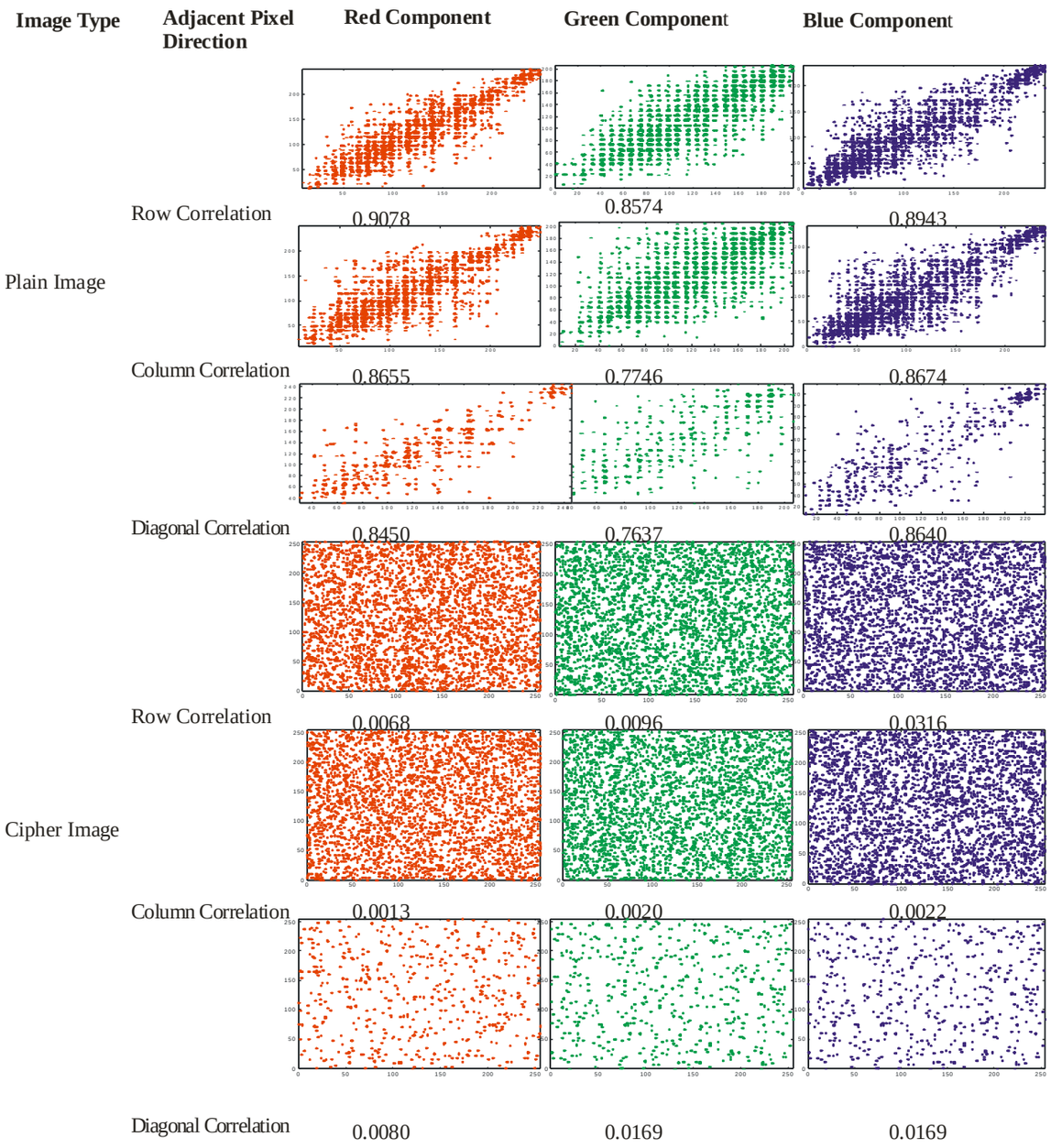


Figure 5: Correlation between adjacent pixels of the plain and the cipher colour image of Mandril using the **Aizawa** chaotic image encryption algorithm.

Performance Analysis Results

The performance of the proposed encryption algorithms was measured using two metrices. The metrices used includes histogram uniformity analysis and the correlation coefficients analysis. The results of the performance analysis for the proposed encryption algorithms are:

Histogram uniformity analysis results

(a) Histogram analysis of the Aizawa chaotic image encryption algorithm on colour image of Lena is shown in Figure 2.

(b) Histogram analysis of the Aizawa chaotic image encryption algorithm on colour image of Mandril is shown in Figure 2.

In figure 2 (a) and (b), it is worthwhile to note that the cithertext image histogram become very flat after encryption. In other words, the cithertext images are random-like. The high information redundancy is one nature of the digital image data and thus it is desired to break the high correlation between neighbour pixels so that the content is not made visible to an intruder.

Correlation coefficient analysis results

(a) Correlation between two adjacent pixels (row, column and diagonal) of plain and cipher colour image of Lena using Aizawa chaotic image encryption algorithm is shown in Figure 4.

(b) Correlation between two adjacent pixels (row, column and diagonal) of plain and cipher colour image of Mandril using Aizawa chaotic image encryption algorithm is shown in Figure 5.

Figure 4 and 5 shows correlation distribution of two adjacent pixels in the plain image and cipher image. It is observed that neighbouring pixels in the plain image are correlated too much, while there is a little correlation between neighbouring pixels in the encrypted image.

Discussion

The Aizawa chaotic image encryption algorithm was proposed. The performance analysis was also carried out on the proposed encryption algorithm using the specified images and the results are shown in Figure 4.

Discussion of the results obtained from the application of the proposed encrption algorithm.

The plain, scrambled, cipher and decrypted colour images of Lena and Mandril using Aizawa chaotic image encryption algorithm are shown in Figure 2 and 3. Visual inspection of the shuffled images from the figures shows how useful the chaotic properties of the Aizawa system are in encrypting images. The decrypted images are as clear as the original images. This shows that the encryption algorithm is effective.

Discussion of the Performance Analysis Results
Discussion of the histogram uniformity analysis result

Figures 2 and 3 show the histograms of the plain,scrambled and encrypted images of Lena and Mandril in the red, green and blue components using the Aizawa chaotic image encryption algorithm. Inspection of the histograms of the encrypted images and that of their original images in all the three colours: red, green and blue show that the corresponding histograms are completely different from each other. Again, a closer look at the histograms of the encrypted images in all the three colours are uniformly distributed. Hence, the proposed algorithm has met the histogram uniformity analysis conditions revealing that the attacker cannot detect any information concerning the plain image from the encrypted image, showing that the cryptosystem is working effectively.

Discussion of the correlation coefficient analysis results

Figure 4 is the result of the correlation coefficient analysis of the Aizawa chaotic image encryption algorithm on colour image of Lena. We can see from the Figure that the plain Lena is highly correlated in red, green and blue components with an average correlation coefficient of 0.9432, 0.9676, 0.8741 along the row, column and diagonal axes respectively.

The cipher Lena has a very low correlation in red, green and blue components with an average correlation coefficient of 0.0089, 0.0184 and 0.0254 along the row, column and diagonal axes respectively that is almost zero. This clearly show that the proposed algorithm is effective.

In Figure 5, we have the result of the correlation coefficient analysis of the Aizawa chaotic image encryption algorithm on colour image of Mandrill. We observe from the result that the plain Mandrill is strongly correlated with minimum correlation coefficient of 0.8865 in the red component, 0.8358 in the green component and 0.8242 in the diagonal axes of the plain Mandrill image. Similarly, we can see from the same figure that the cipher image of the Mandrill has a very low correlation. In the red component, we have a minimum correlation coefficient of 0.0160, 0.0018 and 0.0139 in the red, green and blue components of the Mandrill cipher image respectively. The efectiveness of this algorithm is demonstrated in the fact that the attacker has no information about the plain image since there is no clue to the attacker from the cipher image.

Table 1: Correlation coefficient analysis results of some chaotic methods in the literature and our proposed chaotic methods on a 256x256 image for the purpose of comparison.

Method	Plain Image			Cipher Image		
	Row	**Column**	**Diagonal**	**Row**	**Column**	**Diagonal**
Aizawa chaotic image encryption algorithm-Lena	0.9188	0.9500	0.9239	0.0015	0.0258	0.0371
Aizawa chaotic image encryption algorithm-Mandril	0.8943	0.8674	0.8640	0.0316	0.0022	0.0169
Effa *et al.* 2014.- Lena	0.9333	0.9121	0.8666	-0.0001	-0.0005	-0.0017
Fu *et al.* 2012 –Lena	0.9404	0.9299	0.9257	0.0088	-0.0087	-0.0060
Radha and Venkatesulu (2012)	0.9845	0.9978	0.9712	0.0107	0.0239	0.0348
Amber (2015) –Lena	0.9703	0.9425	0.9188	-0.0013	-0.0274	-0.0199
Yakubu and Aboiyar (2017)-Lena	0.9594	0.9735	0.9333	-0.0043	0.0061	-0.0018

Conclusion

In this paper, the Aizawa chaotic image encryption algorithm was presented. The Aizawa chaotic image encryption algorithm was tested on colour images of Lena and Mandrill and their results ontained. Standard images of Lena and Mandrill of size 256x256 stored in tif format were used as inputs. Two metrics were used in evaluating the performance of the proposed algorithms, the histogram uniformity analysis and the correlation coefficient analysis, results were presented.

The Aizawa chaotic image encryption algorithm has satisfied the conditions of the histogram uniformity analysis and the correlation coefficient analysis of the proposed algorithm on colour images, hence achieving the required level of security.

The simulation results show that the proposed chaotic image encryption algorithms has high operation efficiency and good encryption effect. We therefore conclude that the Aizawa chaotic image encryption algorithms can withstand various forms of attacks ensuring for confidentiality and security. Thus, the new map is suitable for image encryption and can be used for real time applications.

References

Al-Maadeed, S., Al-Ali, A., and Abdalla, T. (2012). A New Chaos-Based Image-Encryption and Compression Algorithm. *Journal of Electrical and Computer Engineering.* 11:201-210.

Auyporn, W. and Vongpradhip, S. (2015). A Robust Image Encryption Method Based on Bit Plane Decomposition and Multiple Chaotic Maps. *International Journal of Signal Processing Systems.* 3 (1):8-13.

Baker, G.L. and Gollub, J.P. (1990). *Chaotic Dynamics an Introduction*. New York: Press Syndicate of the University of Cambridge. 550pp.

Biswas, R.H. (2013). One Dimensional Chaotic Dynamical Systems. *Journal of and Applied Mathematics: Advances and Applications. 10(1)*:69-101.

Guanghui, C., Kai, H., Yizhi, Z., Jun, Z. and Xing, Z. (2014). Chaotic Image Encryption Based on Running-Key Related to Plaintext. *The Scientific World Journal*. 20(14): 9-22.

Jastrzebski, K. and Kotulski, Z. (2009). On Improved Image Encryption Scheme Based on Chaotic Map Lattices. *Engineering Transactions.* 57(2):69-84.

Kaur, S. and Gupta, D. (2016). A Review of Image Encryption Schemes Based on the Chaotic Map. *International Journal of Computer Technology and Applications.* 5(1):144-149. Retrieved from www.ijcta.com on 1st March, 2017.

Kumar, R.R., Sampath, A. and indumathi, P. (2015). Enhancement and Analysis of Chaotic Image Encryption Algorithms. *Journal of Computer Science and Information Technology*. 1:143-152.

Kumaur, N., Wadhwa, D., Tower, D. and Vijayalakshmi, S. (2015). Review of Different Chaotic Based Image Encryption Techniques. *International Journal of Information and Computation Technology*.4(2): 197-206. Retrieved from http://www.irphouse.com/ijict.htm on 2nd March, 2017.

Li, C., Li, S., Alvarez, G., Chen, G. and Lo, K. (2007). Cryptanalysis of Two Chaotic Encryption Schemes Based on Circular bit Shift and XOR Operations. *Physics Letters A.*369*:*23-30.

Li, S., Zheng, X., Mou, X. and Cai, Y. (2015). Chaotic Encryption Scheme for Real-Time Digital Video. *Proceedings of SPIE.* 4666: 149-160.

Liu, H., Kadir, A. and Nu, Y. (2014). Chaos-Based Color Image Block Encryption Scheme Using S-Box. *AEU-International Journal of Electronics and Communications.* 68 (7):676-686.

Mankar, V.H. and Mishra, M. (2011). Chaotic Encryption Using 1-D Chaotic Map. *International Journal of Communications, Network and System Sciences.* 4: 452-455.

Misra, A., Gupta, A. and Rai, D. (2011). Analysing the Parameters of Chaos Based Image Encryption Schemes. *World Applied Programming.* 1(5):294-299.

Pande, A. and Zambreno, J. (2011). A Chaotic Encryption Scheme for Real-Time Embedded Systems: Design and Implementation. *Telecommun Syst*.10: 482-492.

Radha, N and Venkatesulu, M. (2012). A Chaotic Block Cipher for Real-Time Multimedia. *Journal of Computer Science.* 8(6):994-1000.

Sankaran, K.S. and Krishna, B.V. (2011). A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images. *IJIET.* 1(2):137-141.

Telem, A.N.K., Segnin, C.M., Kenne, G. and Fotsin, H.B. (2014). A Simple and Robust Gray Image Encryption Scheme Using Chaotic Logistic Map and Artificial Neural Network. *Advances in Multimedia.* 14(7):1-13.

Wang, X., Lui, L. and Zhang, Y. (2015). A Novel Chaotic Block Image Encryption Algorithm Based on Dynamic Random Growth Technique. *Optics and Lasers in Engineering.* 66(14): 10-18.

Xiao-Jun, T., Zhu, W. and Ke, Z. (2012). A Novel Block Encryption Scheme Based on Chaos and an S-Box for Wireless Sonsor Networks. *Chinese Physics.* 21(2). 287-297.

Yakubu, H.J. and Aboiyar, T. (2017). A Chaos Based Image Encryption Algorithm Using Shimizu-Morioka System. *Information Technology Innovation for Sustainable Development* 28: 77-85.

Zang, T. and He, L. (2001). Chaos-Based Random Number Generators-Part 1: Analysis [Cryptography]. *Circuits and Systems 1: Fundamental Theory and Applications, IEEE Transactions.* 48(3):281-292.

Zhang, W., Tang, S., Zhang, L., Ma, Z. and Song, J. (2015). Chaotic Stream Cipher-Based Secure Data Communications over Intelligent Transportation Network. *International Journal of Antennas and Propagation.* 20(5): 10-21.

Zhe, Z., Haibing, Y., Yu, Z., Wenje, P. and Yupeng, Z. (2010). Block Encryption Scheme on 3 D Chaotic Arnold Maps. *Intelligent Interaction and Effective Computing.* 9(3):47-60.