Pertanika J. Sci. & Technol. 26 (2): 599 - 614 (2018)

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

An Efficient Method for Secure 2D Image Visualization and Transmission through Chaotic Confusion and Pixel Diffusion

Gunasekaran, G.[1]* and Venkatesan, M.[2]

[1]*School of Information Technology and Engineering, VIT University, Vellore-632014, India*

[2]*School of Computer Science and Engineering, VIT University, Vellore-632014, India*

ABSTRACT

The main goal of this paper is to present an efficient method for secure 2D image visualisation and transmission through chaotic confusion and pixel diffusion methods. In recent years, the expeditious valuation of digital data exchange has become very important. The safety of any data exchange is imperative in the digital image data storage, retrieval process and communication procedure. The safety and security issues related to Internet banking and email systems necessitate text security in today's digital media. In order to provide secure transmission and retrieval of image data, pixels in an image are scrambled and replaced within the image. The proposed system uses chaotic confusion and pixel diffusion techniques for securing input images. In the confusion method, the pixels within the image are substituted with other values and in the diffusion method, the pixels are re-substituted within the input image. The confusion method and the diffusion method use the selective technique for the generation of secret keys. Improve the quality of the proposed work is utilizing various image quality parameters and error metrics such as MSE, SNR, PSNR etc. The proposed system also utilises chaos maps for the encryption and decryption of the input image.

Keywords: Confusion and diffusion, cryptography, decryption, encryption

INTRODUCTION

The two basic types of cryptography, symmetric key and asymmetric key, encode image data so that they are unreadable without a secret key to unlock the data (Singh et al., 2015; Hashim & Neamaa, 2014). Faster creation and evaluation of digital data sharing is a current need. At the present time, a more secure data transmission process is being sought as security is a very important requirement in the process of data storage and transmission. All transactions through Internet banking and online systems such as m-commerce,

Article history:
Received: 15 September 2017
Accepted: 9 March 2018

E-mail addresses:
ggunasekaran@vit.ac.in (Gunasekaran, G.)
mvenkatesan@vit.ac.in (Venkatesan, M.)
*Corresponding Author

ISSN: 0128-7680 © 2018 Universiti Putra Malaysia Press.

e-business and e-shopping as well as the use of email systems require effective and efficient security. Digital image security is also crucial and must be effectively utilised during digital image transmission and storage; this is a crucial need in industry and research. A systematic method to develop federal data handling standards that are more powerful, adaptable, secure and fast in replacing the basic information encryption standard has been initiated by the National Institute of Standards and Technology, Gaithersburg, Maryland, United States. Digital images have a large data size and also introduce real-time problems. Current methodologies cannot be utilised to safeguard digital images or text data from illegal access, but with a few amendments to the AES method, these can be effectively safeguarded. The various encryption-decryption techniques used for security purposes are symmetric cryptosystems, DES, AES, Blowfish and RSA (Mitali & Sharma, 2014). Comparatively, symmetric cryptosystems are faster than other methods and only a system that has the key can decrypt the received data. The disadvantage of symmetric cryptosystems is that they have transportation issues; in addition, digital signatures cannot be provided. Data Encryption Standard (DES) is proven to be unaffected by all types of cryptanalysis. Since DES has a very small key size, it takes less time to be searched. In general, the AES method is resistant to almost all known attacks and is fast and flexible. However, the key required in the AES method is too large, and this makes computation complex. Compared with other methods, RSA provides better security. It is also capable of providing digital signatures. The processing of public key cryptography is very slow, and this is the disadvantage of this system. The proposed work presents an effective encryption and decryption method for digital images utilising a selective approach for securing the image data to overcome unauthorised access. It also overcomes the disadvantages that remain with the existing system.

RELATED WORK

This section discusses various works related to the field of digital transmission that uses suitable techniques for encryption and decryption of digital images. Cryptography is considered a branch of both mathematics and computer science that associates closely with information theory and coding methods, computer security, computer engineering and commerce. Many studies have been done on image encryption to meet the need for real-time safe digital image communication and transmission over the web by means of wireless communication networks. This paper focusses on efficient techniques for secure 2D image visualisation and transmission through chaotic confusion and pixel diffusion. Several previous works have been consulted for help in developing the proposed system. A fast encryption method based on vector quantisation is proposed for image security. A comparison is made by integrating diffuse codes to confuse the code concepts and to encrypt the elements of the security book using a symmetric security algorithm (Chang et al., 2001). An unreachable differential security analysis of AES-192 and AES-256 (Phan, 2004) up to sound rounds is proposed.

Selective encryption is a new technique that reduces computational complexity. Selective encryption improves a simple scalar quantised sample to illustrate the influence of the basic components, list out various essential consumer electronic equipment and use a suitable method for improving and examining selective encryption for specific compression methods

(Lookabaugh & Sicker, 2004). A study motivated and background that by the different standard and developed magnification lens rendering methods to magnify the topographic of interest, whereas compressing the outstanding volume areas without removing them left entirely are presented (Wang et al., 2005). All our lenses are accelerated on the GPU. In this method, the user accesses the obtainable screen region interactively, and is offered more regions with the best resolution and essential features. A simple technique for image security utilising an integration of block-based image transformation and encryption was proposed by Bani et al. (2008). Their proposed method provided good performance in terms of correlation and entropy calculations compared with the existing methods. A novel crypto-system for encrypting and decrypting digital images, audios and videos was presented. Associations with confusion and diffusion behaviours by utilizing chaotically coupled chaotic maps were proposed and described by Pisarchik and Zanin (2008). Their proposed scheme was more secure than existing methods in terms of computational speed, content security and improved speed of transmission between sender and receiver.

Wang et al. described cross chaotic maps that aid logistic maps and Chebyshev maps (2008). Here, every pixel in the image is randomly moved according to the encryption matrix in the process of grayscale substitution. In addition, the scrambling process is applied in the process of position permutation. The development of digital information coding based on the combination of chaotic techniques was presented by Behnia et al. (2008). Here, the combination of chaotic maps illustrates the merits of large key space and higher-end security. Also, the proposed method presented an idea for practical utilisation of security in the secure communication of personal data over the network. The proposed advanced Hill cipher secure technique was highly secure against brute force attacks when compared with original Hill cipher technique (Acharya et al., 2009). A new image coding method to support both abstract analysis and practical solutions representing high-end security was proposed by Wei-Bin and Xin (2009). The proposed method had many advantages such as support for a lot of key space, shorter running time compared with other methods and a very sensitive secret key. An advanced encryption standard to develop a secure symmetric image encryption method was presented by Kamali et al. (2010). Their work utilised row-changing alteration. Verma et al. did a comparative analysis of four commonly used techniques and presented their analysis (2011). Their work presented the possibility of faster digital transmission and a higher level of security through strong key size functions, random bit creation and Internet-based systems. On their part, Shazmeen and Prasad (2012) showed a new cryptographical approach that aids symmetric cryptography in combination of a software-based security system. The main objective was to provide better transmission security for banking customers. Their proposed work also described existing online banking issues and identified the requirement for security performance for online banking systems. Comparative performance analyses of selected symmetric cryptography methods were presented.

Selected methods such as AES, DES, 3DES, RC6, Blowfish and RC2 were demonstrated by Mathur and Kesarwani (2013). They presented experimental results related to encoding, packet size and data types. The best hybrid models for image encryption based on a genetic algorithm through chaotic function were discussed by Nichat and Sikch (2013). In their work, images were converted from plain text to cipher text with the help of the chaotic method

using a secret key and in the second step, the genetic algorithm was applied for optimising the conversion of ciphered text to the encrypted form effectively. The experimental results compared the correlation components and entropy value. Encryption and decryption methods were proposed based on a chaotic map to create a permutation matrix with two parameters to create a shuffler. The proposed method's key space was huge enough to attack all types of brute-force attacks (Bremnavas et al., 2013). The experimental results suggested that this method was a good candidate for image operation for cryptography and steganography. A selective image encryption method for medical and satellite images was presented by Panduranga and Naveenkumar (2013). The first method for selective encryption was valuable for cases where the region or location of interest is known. The second method for selective encryption was important for instances where concentrated objects appear in one image. Another selective image encoding method that contains extreme image information was described by Ullah et al. (2013). The proposed work can be applied to encrypt medical images because medical image information also requires higher-level security for image transfer through unauthorised channels. Efficient and highly secure methods are used for image encryption (Gunasekaran & Ray, 2014). The results and discussion showed that a high level of security using the image encryption method with less computational time was ensured. The study helped to increase security levels for medical and non-medical images that are illustrated. Hashim and Neamaa (2014) used the modified Elgamal cryptosystem method to support both colour and black and white images of any size stored in PNG and JPG formats for encrypting and decrypting with the help of revised cryptosystems. The modified Elgamal system provides more security than other methods. Mitali and Sharma (2014) did a comparative study of different security methods on several settings of information packets. Their paper investigated different types of encryption and decryption to provide better encryption methods with higher computational speed and to reduce energy consumption. A new scheme for image encryption and verification for digital transmission was introduced. Many chaos-based image encoding methods were presented by Thakur et al. (2014). The created hash function was embedded in the image and the whole image was encoded with a mixture of chaotic maps and substitution diffusion methods were presented. Various symmetric cryptography methods such as AES, DES, 3DES, Blowfish, RC4 and RC6 were demonstrated and reviewed by Princy (2015). Finally, the author suggested that the blowfish method was more secure compared with other cryptography methods and showed good experimental outcomes for low computational cost and a fewer number of rounds. An advanced multi-level secret sharing visualising cryptography method for encapsulating information in colour image and its respective share was illustrated as captcha to customers. Phishing websites, as well as human user attacks, can be easily monitored and resolved, as demonstrated by Priya et al. (2015). The proposed technique provided multi-level verifications and validation processing by captcha options. Two-dimensional Henon chaotic maps and skew tent maps were arranged in a scheme for effective chaos-based image encryption methods by Khan et al. (2015). Confusion and diffusion methods were applied for encryption and decryption of images; chaotic maps play a key role in permutation and diffusion machines. The method can be easily used for unbalanced images that have a different width and height as well. An efficient coding technique for encoding and decoding images with the help of symmetric key concepts were illustrated by Singh et al. (2015). The advantage is that the proposed system

used a separate key that was required for both the sender and the receiver. This cryptosystem key concept helped in sending a huge volume of messages. Other techniques for computer networking and various loopholes in current network systems were analysed by Ruman and Phaneendra (2015). The various security threads overtaken by different technologies for securing the network through cryptography and encryption methods were presented. A proposed method utilising an enhanced RSA method was proposed. It also improved the number of bits in the SSL connection for security. This method guaranteed secure service compared with other systems in terms of key creation time. An innovated image encryption method created on a Henon map and complex spatiotemporal chaos methods were presented by Zheng and Jin (2015). The work focused on pixel location permutation and pixel position shifting, which help the cryptosystem. The blowfish method developed and implemented with help of the WDDL logic pattern in a bottom-up fashion was projected by Dinesh and Suveetha (2016). A separate secure key was used for encryption and decryption by both the sender and receiver without modification of the source image and encrypted image. Various other efficient methods and techniques helped to develop secure 2D-image visualisation and digital transmission through the chaotic confusion and pixel diffusion methods. This proposed work concentrated on an encryption and decryption model using the selection approach with association with the Hundugen function for generating a secret key.

PROPOSED ENCRYPTION AND DECRYPTION METHOD

The proposed work on encrypting and decrypting digital images using the selective approach is shown in Figure 1. Security can be applied to the image data that are sent through the web or any other communication medium in the network. The proposed work ensures security so that nobody can have unauthorised access to the digital resources that need to be protected. The proposed system used the permutation combination technique to encrypt the input digital image and thereby, lock the private key. Anyone who has the key will have the privilege of accessing a particular image. In the encryption model of the image security system, the confusion technique was utilized, whereas in the decryption model, the diffusion technique (Pisarchik & Zanin, 2008; Ling et al., 2008) was utilised for its efficacy. The overall architecture had two levels of encoding: the image encryption model and the image decryption model. The image encryption model will import any type of image with a private key and encrypt the input image into a cipher code form, while the image decryption model decrypts the encrypted image and reports back to the original image. The following diagrammatical representation shows the encryption and decryption systems using the selective approach method.

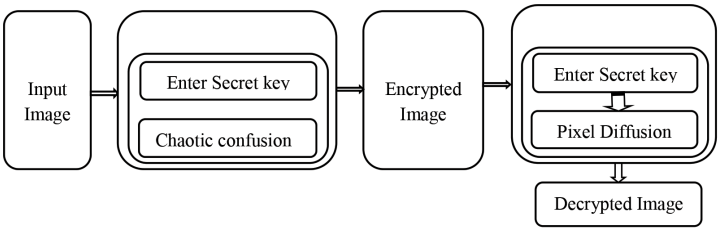


Figure 1. Overall architecture of encryption and decryption systems

The three major processes involved in the proposed method are as follows. First, the input image is read into the encryption model through the selective encryption approach. Second, the process of key generation is described; here, the primary key is generated (Acharya et al., 2009). Finally, the Hundungen process is executed to generate a Henon map by generating random numbers to decrypt the encrypted image. The Henon map is a discrete-time dynamical system that exhibits chaotic behaviour (Khan et al., 2015). Once the input image is provided, the key is generated in the developed system. The generated key acts as the password and locks the input image until the correct image is provided. Then, the key generation function is executed automatically, and all four keys K1, K2, K3 and K4 are calculated. Once the Hundungen function is executed, it manipulates the images pixel by pixel and then encrypts the image by manipulating the pixels within the image. Chaotic confusion is an encryption technique that shuffles the pixels within an image or substitutes the pixels within an image. Pixel diffusion is another encryption technique in which the pixels in an image will be replaced with the XORed values of the RGB components. The key approaches involved in the encryption and decryption are as follows.

Selective Encryption Approach

Selective encryption is a technique to save computational complexity or enable interesting new system functionality by only encrypting a portion of the image while still achieving adequate security (Lookabaugh & Sicker, 2004). The selective encryption approach connects all other models in the system and will run as the main function in the system process. Once the input image is read from the user, the respective key has to be submitted to the system to encrypt and lock the image. Then, its Red (R), Green (G) and Blue (B) values are taken, and the Hundungen function is executed to generate various keys to encrypt the image so that the original image cannot be viewed by any unauthorised users. If the image is to be decrypted, then the person who is accessing it has to provide the correct key to view the original image. The image is decrypted back again using the key-gen function, which will reverse the process from the end of the encryption and return the original image as the final one. The histogram of the image gives the number of intensity values that are present in a particular image. The histograms of the input image and the decrypted image are compared to determine the visual efficiency of the decryption. In the proposed work, the chaos-based image encryption scheme was suggested; the scheme involved two different processes, chaotic confusion and pixel diffusion (Pisarchik & Zanin, 2008; Ling et al., 2008). Chaotic confusion is the process of transforming to the cipher image from the plain image. In this proposed method, the confusion process was performed by bitXORing, the first pixel of the red channel of the image with the key, K_1, the first pixel of the green channel with K_2 and the first pixel of the blue channel with key K_3 and the other pixels were XORed.

$$R(1,1) = R(1,1) \text{ XOR } K_1 \quad [1]$$

$$G(1,1) = G(1,1) \text{ XOR } K_2 \quad [2]$$

$$B(1,1) = B(1,1) \text{ XOR } K_3 \quad [3]$$

$$R(1,2) = R(1,2) \text{ XOR } K_4 \quad [4]$$

The process is repeated until all the pixels of the R, G and B components are XORed. After the chaotic confusion process, the pixel diffusion process is executed. In this pixel diffusion process, the output bit values should depend on the input bit of values in a very difficult way. To achieve this, the pixel diffusion process was carried out in two steps i.e. horizontal diffusion and vertical diffusion.

The proposed algorithm was as follows.

Algorithm 1: Selective Approach Encryption

Start
Step 1: Read the input image, I.
Step 2: Input the private key, K, into the encryption model.
Step 3: Generate RGB components from the input image.
Step 4: Calculate Henon map, $X_{n+1}= Y_{n+1}-aX^2_{n,}$ $Y_{n+1}=bX^2_{n,\text{ and}}$ $Z_{n+1}=1-cY^2_{n+1}+X_{n.}$
Step 5: Bit-XOR the private key, K, with all the RGB components of the input image.
Step 6: Substitute with the XOR-ed pixels into one to form the cipher image.
Step 7: Encrypted image $I_{\text{Encr is}}$ generated.
Stop

Algorithm 2: Selective Approach Decryption

Start
Step 1: Read the encrypted image, $I_{\text{Encr.}}$.
Step 2: Generate random numbers, Rnd = $\{(X_1, Y_1, Z_1), (X_2, Y_2, Z_2). . ., (X_n, Y_n, Z_n)\}$
Step 3: Generate Henon map using random numbers.
Step 4: Enter the private key, K.
Step 5: Bit-XOR the random numbers, Rnd, with the original input image, I.
Step 6: Compare the results of the previous step with the results of step 3 in the encryption algorithm.
Step 7: If the two results match, re-substitute the original pixels to obtain the decrypted image, I_{Decr}.
Step 8: If the results do not match, perform step 3 to step 5; otherwise,
Stop

Hundungen function

The Henon map is utilised for image encryption in the proposed method. The Henon map is used to represent the disconnected time dynamic system, which is a mathematical concept in which a fixed rule describes the time dependence of a point in a geometric space. The Henon map is defined by the function:

$$X_{n+1}= Y_{n+1}-aX^2_n \quad [5]$$

$$Y_{n+1}=bX^2_n \quad [6]$$

$$Z_{n+1}=1-cY^2_{n+1}+X_n \quad [7]$$

where, a, b and c are constants and X, Y and Z are pixel colours for each channel like Red, Green and Blue, respectively. This function generates a random value, and these random values are bitXORed with the original value of the image i.e. the X value will be bitXORed with the red channel pixel, Y with the green channel and Z with the blue channel. Image encryption using the chaos map includes the input image and the secret key for encrypting the plain image. The first step will be to generate the keys, which will consist of the four variables K_1, K_2, K_3, and K_4. The values of X_n, Y_n and Z_n will be generated using the Henon map function, which will be used to generate the key. The K_1 key will be generated by multiplying the values of X_n and Y_n and dividing the result by 256. The K_2 key will be generated by multiplying the values of Y_n and Z_n and dividing the result by 256, and the K_3 key will be generated by multiplying the values of Z_n and X_n and dividing the result by 256. The K4 key will be generated by taking the mod of X_n and 256. The keys will be generated by the following rules:

$$K_1= (X_n*Y_n)/256 \quad [8]$$

$$K_2= (Y_n*Z_n)/256 \quad [9]$$

$$K_3= (Z_n*X_n)/256 \quad [10]$$

$$K_4=\text{mod}\ (X_n, 255) \quad [11]$$

Key Generation Function

The keys are generated in the reverse manner from which the Hundungen function is executed because the values of the matrix at the same positions of the original image have to be reversed. Once the correct key is provided, then the values of all the respective keys are calculated and checked. Then, these keys are bitXORed to calculate the values of the matrix pixel by pixel. The processes of chaotic confusion and pixel diffusion are reversed, and each pixel value is the same as that of the original image pixel value.

RESULTS AND DISCUSSION

Several different types of digital image with a size of 256*256 are utilised to demonstrate the encryption and decryption of images in the proposed system. A sample of five different images is considered and projected here, and the quality measures and error metrics of the images are calculated to determine the efficiency of the proposed system. Table 1 shows the empirical results and the elapsed times that are obtained from the developed system. The various quality

measurements for the encrypted and decrypted images are projected from Tables 2 and 3, and the error metrics for both the encrypted and decrypted images are illustrated from Tables 4 and 5. A graphical representation of the elapsed time for processing the encrypted and decrypted images is depicted in Figure 2.

Table 1
Experimental results for input, encrypted and decrypted images

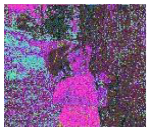
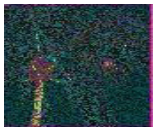
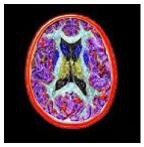
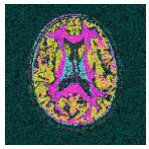
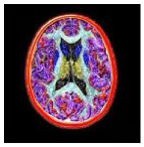
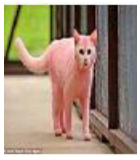
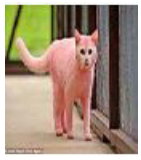
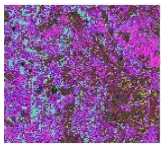
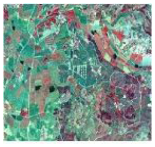
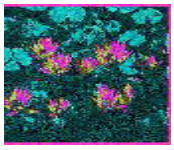
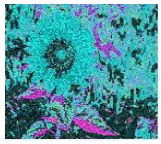
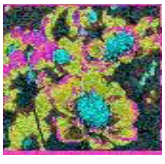
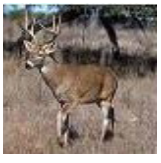
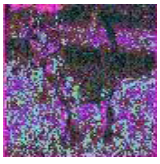
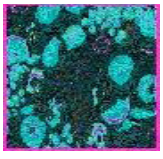
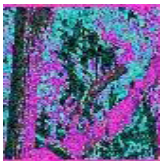
Sl. No.	Input Image	Encrypted Image	Decrypted Image	Sl. No.	Input Image	Encrypted Image	Decrypted Image
1				7			
2				8			
3				9			
4				10			
5				11			
6				12			

Table 1 (*continue*)

Sl. No.	Input Image	Encrypted Image	Decrypted Image	Sl. No.	Input Image	Encrypted Image	Decrypted Image
13				18			
14				19			
15				20			
16				21			
17				22			
23				24			

The comparison of various encryption and decryption methods is shown in Table 6 and Table 7. The data encryption standard method attained a maximum entropy of 8.25, whereas the proposed method managed to attain 7.25 and the data decryption standard method attained a maximum entropy of 8.75, whereas the proposed method managed to attain 7.75, which was the least among the other methods. Maximum entropy represents the maximum disorder and the minimum entropy represents the minimum disorder of data. Thus, the proposed system developed provides a better means of secured transmission of data.

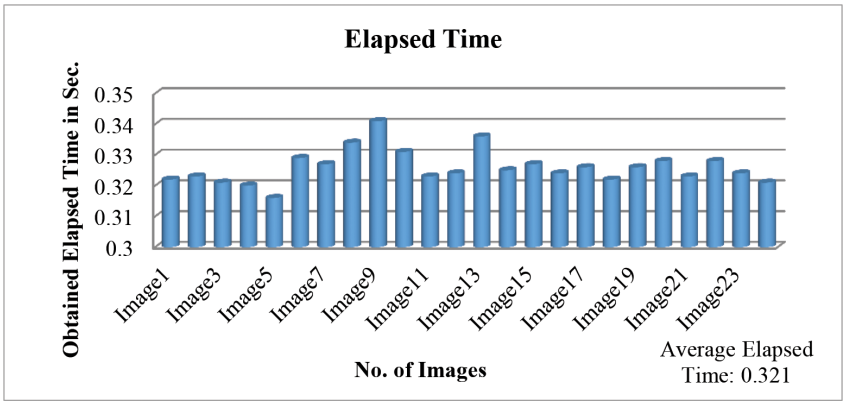


Figure 2. Graphical representation of elapsed time achieved for the input images

Table 2

Image quality measures between input image and encrypted images

Sl. No.	MSE	PSNR	MNCC	AD	SC	MD	NAE
Image 1	41.49	15.77	0.93	16.82	1.10	220	0.10
Image 2	40.23	16.04	0.98	-7.23	1.00	237	0.12
Image 3	45.85	14.90	1.00	-10.99	0.94	173	0.14
Image 4	36.92	16.78	0.94	13.54	1.07	222	0.09
Image 5	34.10	17.48	0.96	8.07	1.06	250	0.08
Image 6	42.05	15.65	0.94	3.80	1.06	224	0.12
Image 7	46.79	14.73	0.92	17.80	1.11	236	0.12
Image 8	30.56	18.42	0.98	-2.50	1.01	252	0.08
Image 9	29.93	18.60	0.98	5.97	1.02	181	0.08
Image 10	43.30	15.40	0.92	18.97	1.12	236	0.11
Image 11	33.20	17.70	0.98	-0.06	1.01	205	0.09
Image 12	52.05	13.80	0.89	23.76	1.19	245	0.14
Image 13	65.20	11.84	0.84	37.48	1.29	236	0.16
Image 14	43.86	15.29	0.91	23.48	1.16	175	0.11
Image 15	44.39	15.18	0.927	17.72	1.12	248	0.11
Image 16	82.69	9.78	0.80	46.38	1.39	247	0.21
Image 17	35.86	17.03	0.99	-1.58	0.99	220	0.10
Image 18	38.19	16.49	0.99	-5.42	0.96	198	0.11
Image 19	33.76	17.56	0.962	10.45	1.07	221	0.09
Image 20	47.28	14.63	0.926	16.29	1.12	238	0.12
Image 21	36.49	16.89	0.954	12.02	1.07	228	0.10
Image 22	46.87	14.71	0.905	19.01	1.16	217	0.12
Image 23	28.78	18.94	0.989	2.34	1.03	239	0.08
Image 24	34.38	17.40	0.95	12.89	1.08	235	0.09

MSE: Mean Squared Error; PSNR: Peak Signal-to-Noise Ratio; MNCC: M-Normalized Cross-Correlation; AD: Average Difference; SC: Structural Content: MD: Maximum Difference: NAE: Normalized Absolute Error

Table 3
Image quality measures between encrypted and decrypted images

Sl. No.	MSE	PSNR	MNCC	AD	SC	MD	NAE
Image 1	41.49	15.77	1.03	-16.81	0.90	207	0.11
Image 2	40.22	16.04	0.98	7.23	0.99	254	0.12
Image 3	45.85	14.90	0.94	10.99	1.06	253	0.12
Image 4	36.92	16.78	1.02	-13.54	0.92	180	0.10
Image 5	34.10	17.47	1.01	-8.07	0.94	182	0.08
Image 6	42.05	15.65	1.01	-3.80	0.93	202	0.12
Image 7	46.79	14.72	1.03	-17.80	0.89	190	0.13
Image 8	30.56	18.42	0.99	2.50	0.99	145	0.08
Image 9	29.93	18.60	1.00	-5.97	0.97	158	0.08
Image 10	43.30	15.40	1.04	-18.97	0.89	185	0.12
Image 11	33.20	17.70	0.99	0.06	0.98	197	0.09
Image 12	52.04	13.80	1.06	-23.76	0.84	173	0.16
Image 13	65.20	11.84	1.09	-37.48	0.77	103	0.19
Image 14	43.86	15.29	1.05	-23.47	0.86	111	0.13
Image 15	44.39	15.18	1.039	-17.72	0.89	168	0.12
Image 16	82.69	9.78	1.11	-46.38	0.71	189	0.26
Image 17	35.86	17.03	0.98	1.58	1.01	203	0.09
Image 18	38.19	16.49	0.97	5.42	1.02	178	0.10
Image 19	33.76	17.56	1.01	-10.45	0.93	164	0.09
Image 20	47.28	14.63	1.03	-16.29	0.89	191	0.13
Image 21	36.49	16.89	1.01	-12.01	0.93	189	0.10
Image 22	46.87	14.71	1.05	-19.00	0.86	188	0.14
Image 23	28.78	18.94	1.00	-2.34	0.97	170	0.07
Image 24	34.37	17.40	1.02	-12.89	0.92	163	0.09

Table 4
Error metric measurement for original images

Sl. No.	SNR	RMSE	UIQI	EME1	EME2	PCC1	PCC2	MAE
Image 1	-5.78	31.05	0.63	25.46	6.16	16704.49	19879	6.45
Image 2	-9.98	35.30	0.54	26.72	7.39	17749.23	19879	6.07
Image 3	-5.58	30.14	0.41	13.59	5.01	17035.99	19739	5.89
Image 4	-5.40	29.73	0.65	22.16	5.05	16058.24	20303	6.17
Image 5	-6.08	31.80	0.61	30.82	8.41	39404.04	44943	6.39
Image 6	-8.31	33.66	0.57	41.63	9.11	8158.30	8857	5.62
Image 7	-6.11	32.11	0.58	28.97	6.24	8009.28	9047	6.45
Image 8	-7.83	36.04	0.44	48.97	12.64	7221.16	8943	6.55

Table 4 (*continue*)

Sl. No.	SNR	RMSE	UIQI	EME1	EME2	PCC1	PCC2	MAE
Image 9	-5.95	31.13	0.41	21.20	3.27	7207.68	8735	6.55
Image 10	-5.75	30.80	0.57	31.49	10.99	7726.37	8797	6.08
Image 11	-7.00	33.41	0.70	64.75	12.08	7409.20	8669	6.47
Image 12	-6.63	33.24	0.64	36.94	8.80	7931.42	8669	6.26
Image 13	-6.86	35.18	0.46	7.62	1.98	6653.55	8834	6.42
Image 14	-6.01	31.92	0.42	9.89	2.52	7510.33	9029	6.43
Image 15	-6.30	32.87	0.57	29.29	6.21	8044.06	9063	6.59
Image 16	-7.49	37.73	0.42	15.39	3.22	11470.84	13224	6.20
Image 17	-5.76	30.82	0.67	30.46	8.94	7122.60	8548	6.26
Image 18	-5.44	29.86	0.43	19.95	6.96	7362.12	8631	6.03
Image 19	-6.88	34.89	0.69	44.47	7.28	7602.61	8924	7.49
Image 20	-6.37	32.96	0.80	49.59	7.71	8119.59	9029	6.53
Image 21	-5.57	30.24	0.54	28.28	11.23	7145.53	8599	6.20
Image 22	-6.48	32.65	0.64	44.46	10.06	8078.24	8839	6.04
Image 23	-6.32	32.72	0.53	36.34	10.00	7508.96	8651	6.14
Image 24	-5.87	31.33	0.68	34.15	6.01	7180.56	8669	6.59

SNR: Signal-to-Noise Ratio; RMSE: Root Mean Squared Error; UIQI: Universal Image Quality Index; EME1 (Original Image): Measurement of Enhancement; EME2 (Encrypted Image); PCC1 (Original Vs Noise): Pearson Correlation Coefficient; PCC2 (Original Vs Original): Pearson Correlation Coefficient; MAE: Mean Absolute Error

Table 5
Error metric measurement for encrypted images

Sl. No.	SNR	RMSE	UIQI	EME1	EME2	PCC1	PCC2	MAE
Image 1	-5.44	29.86	0.74	38.32	8.72	16135.62	19599	5.96
Image 2	-6.16	32.38	0.58	39.92	9.42	16832.39	19737	6.18
Image 3	-5.97	31.72	0.63	26.22	5.39	16856.93	19739	6.74
Image 4	-5.62	30.50	0.75	32.07	7.41	16334.77	20019	6.31
Image 5	-5.71	30.81	0.64	30.39	6.95	36983.29	44729	6.49
Image 6	-6.61	33.98	0.58	47.56	8.11	6440.08	8414	6.59
Image 7	-5.59	30.24	0.73	49.10	15.32	7188.09	8735	5.84
Image 8	-6.34	32.82	0.58	50.79	17.28	5451.67	8567	6.04
Image 9	-5.73	30.74	0.70	43.41	13.26	7593.14	8903	6.16
Image 10	-5.18	28.93	0.69	36.96	16.39	7066.68	8735	5.68
Image 11	-6.19	32.35	0.71	52.20	9.72	7117.01	8903	6.29
Image 12	-5.72	30.73	0.62	36.79	10.47	6672.96	8735	6.34
Image 13	-5.79	31.09	0.58	23.02	6.19	6562.29	9359	6.95

Table 4 (*continue*)

Sl. No.	SNR	RMSE	UIQI	EME1	EME2	PCC1	PCC2	MAE
Image 14	-5.61	30.44	0.61	28.79	7.54	6870.67	9151	6.39
Image 15	-6.13	32.20	0.73	45.07	10.47	7286.15	8988	6.68
Image 16	-5.63	30.52	0.50	26.89	6.88	6033.29	8199	6.77
Image 17	-5.88	31.29	0.78	46.00	8.69	7886.52	9221	6.37
Image 18	-5.81	31.17	0.70	29.80	5.41	7448.92	9047	6.60
Image 19	-6.33	32.99	0.70	47.99	14.47	7516.60	9239	6.76
Image 20	-5.82	31.08	0.78	50.52	9.21	7228.54	8714	6.47
Image 21	-5.56	30.176	0.72	41.24	7.77	7266.09	8857	6.06
Image 22	-5.56	30.23	0.65	32.59	9.18	6553.60	8499	6.40
Image 23	-6.03	31.66	0.69	47.98	9.34	7157.70	8839	6.01
Image 24	-5.18	29.00	0.71	38.55	5.19	6851.51	8857	5.76

Table 6
Comparison of different encryption methods with entropy value

Encryption Algorithm	Entropy Values
DES	8.2525
AES	7.8978
MAES	7.8991
Proposed Method	7.2548

Table 7
Comparison of different decryption methods with entropy value

Decryption Algorithm	Entropy Values
DES	8.7536
AES	8.3978
MAES	8.4002
Proposed Method	7.7559

CONCLUSION

An efficient system for the secure transmission of digital images was developed and presented in this paper. The chaotic confusion and pixel diffusion techniques were utilised for encryption and decryption, respectively. The effectiveness of the developed system was demonstrated based upon the elapsed time between the encryption and decryption of the digital images. A histogram representation showed that there was almost no loss of data during the encryption and decryption processes. Quality measures and error metrics were computed for all the input images, and the results were tabulated. It could be concluded that the developed system ensured that the image data could be transmitted in an effective and efficient manner.

REFERENCES

Acharya, B., Panigrahy, S. K., Patra, S. K., & Panda, G. (2009). Image encryption using advanced hill cipher algorithm. *International Journal of Recent Trends in Engineering, 1*(1), 243–247.

Bani Younes, M. A., & Jantan, A. (2008). Image encryption using block based transformation algorithm. *IAENG International Journal of Computer Science, 35*(1), 407–415.

Behnia, S., Akhshani, A., Mahmodi, H., & Akhavan, A. (2008). A novel algorithm for image encryption based on mixture of chaotic maps. *Chaos, Solitons and Fractals, 35*(2), 408–419.

Bremnavas, I., Poorna, B., & Mohamed, I. R. (2013). Secured medical image transmission using chaotic map. *Elixir Computer Science and Engineering 54*(1), 12598–12602.

Chang, C. C., Hwang, M. S., & Chen, T. S. (2001). A new encryption algorithm for image cryptosystems. *Journal of Systems and Software, 58*(2), 83–91.

Dinesh, M., & Suveetha, D. P. (2016). Real time image encryption and decryption using blowfish algorithm. *International Journal of Emerging Technology in Computer Science and Electronics (IJETCSE), 22*(2), 9–14.

Gunasekaran, G., & Ray, B. K. (2014). Encrypting and decrypting image using computer visualization techniques. *ARPN Journal of Engineering and Applied Sciences, 9*(5), 646–650.

Hashim, H. R., & Neamaa, I. A. (2014). Image encryption and decryption in a modification of ElGamal cryptosystem in MATLAB. *International Journal of Sciences: Basic and Applied Research (IJSBAR), 14*(2), 141–147.

Kamali, S. H., Shakerian, R., Hedayati, M., & Rahmani, M. (2010, August). A new modified version of advanced encryption standard based algorithm for image encryption. In *International Conference on Electronics and Information Engineering (ICEIE), 2010* (Vol. 1, pp. 141–145). IEEE.

Khan, J., Ahmad, J., & Hwang, S. O. (2015). An efficient image encryption scheme based on Henon map, skew tent map and S-Box. In *6th International Conference* on *Modeling, Simulation, and Applied Optimization (ICMSAO), 2015* (pp. 1–6). IEEE.

Lookabaugh, T., & Sicker, D. C. (2004). Selective encryption for consumer applications. *IEEE Communications Magazine, 42*(5), 124–129.

Mathur, M., & Kesarwani, A. (2013). Comparison between DES, 3DES, RC2, RC6, Blowfish and AES. In *Proceedings of National Conference on New Horizons, IT-NCNHIT* (Vol. 3, pp. 143–148). Mumbai, India.

Mitali, V. K., & Sharma, A. (2014). A survey on various cryptography techniques. *International Journal of Emerging Trends and Technology in Computer Science, 3*(4), 6, 307–312.

Nichat, S. P., & Sikchi, S. S. (2013). Image encryption using hybrid genetic algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(1), 427–432.

Panduranga, H. T., & Naveenkumar, S. K. (2013). Selective image encryption for medical and satellite images. *International Journal of Engineering and Technology (IJET), 5*(1), 115–121.

Phan, R. C. W. (2004). Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES). *Information Processing Letters, 91*(1), 33–38.

Pisarchik, A. N., & Zanin, M. (2008). Image encryption with chaotically coupled chaotic maps. *Science Direct, Physical D: Nonlinear Phenomena, 237*(20), 2638–2648.

Princy, P. (2015). A comparison of symmetric key algorithms DES, AES, Blowfish, RC4, RC6: A survey. *International Journal of Computer Science and Engineering Technology (IJCSET), 6*(5), 328–331.

Priya, S., Malathi, M., & Jayaseelan, G. (2015) Secured internet banking using image captcha technique. *Proceedings of International Journal of Emerging Technology and Innovative Engineering, 1*(11), 1–6.

Ruman, K., & Phaneendra, H. D. (2015). Implementation of methods for transaction in secure online banking. *International Journal of Technical Research and Applications, 3*(4), 41–43.

Shazmeen, S. Y., & Prasad, S. (2012). A practical approach for secure internet banking based on cryptography. *International Journal of Scientific and Research Publications, 2*(12). 1–6.

Singh, J., Lata, K., & Ashraf, J. (2015). Image encryption & decryption with symmetric key cryptography using MATLAB. *International Journal of Current Engineering and Technology, 5*(1), 448–451.

Thakur, A., Kumar, R., Bath, A., & Sharma, J. (2014). Design of selective encryption scheme using MATLAB. *International Journal of Electrical & Electronics Engineering, 1*(1), 14–19.

Ullah, I., Iqbal, W., & Masood, A. (2013). Selective region based images encryption. In *2nd National Conference on Information Assurance (NCIA), 2013* (pp 125–128). IEEE.

Verma, O. P., Agarwal, R., Dafouti, D., & Tyagi, S. (2011, April). Performance analysis of data encryption algorithms. In *3rd International Conference on Electronics Computer Technology (ICECT), 2011* (Vol. 5, pp. 399–403). IEEE.

Wang, L., Ye, Q., Xiao, Y., Zou, Y., & Zhang, B. (2008). An image encryption scheme based on cross chaotic map. In *Image and Signal Processing* (Vol. 3, pp. 22-26). IEEE.

Wei-Bin, C., & Xin, Z. (2009). Image encryption algorithm based on Henon chaotic system. In *International Conference on Image Analysis and Signal Processing (IASP), 2009* (pp. 94–97). IEEE.

Zheng, Y., & Jin, J. (2015). A novel image encryption scheme based on Henon map and compound spatiotemporal chaos. *Multimedia Tools and Applications, 74*(18), 7803–7820.