Wireless Pers Commun (2015) 84:901–918
DOI 10.1007/s11277-015-2667-9

An Experimental Comparison of Chaotic and Non-chaotic Image Encryption Schemes

Jawad Ahmad[1] · Seong Oun Hwang[2] · Arshad Ali[3]

Published online: 13 May 2015

Abstract During last few years, transmission of digital multimedia data (images, audios and videos) over Internet, wireless cell phones, television broadcasting etc., has been significantly evolved. The provision of security to store and transmit data with confidentiality, integrity, and authentication for multimedia data over wireless medium is attaining importance these days. Over a few decades, a number of image encryption schemes have been implemented, each with various features, pros and cons. So there is a need to carry out security analysis of these schemes through some standard parameters. In this paper, an effort is being made for comparison of traditional encryption algorithms via some security parameters rather than using just visual inspection. Through these security parameters, one can determine a better and highly secure image encryption scheme. Comparative analysis of Advanced Encryption Standard, Compression Friendly Encryption Scheme, Chaotically Coupled Chaotic Map Encryption Scheme and a Bernoulli Map Based Encryption Scheme are done. Results are finally compiled to conclude the optimum scheme to be used feasibly with high security level.

Keywords Chaos · AES · CFES · MCFES · Image encryption

✉ Seong Oun Hwang
bardic@naver.com; sohwang@hongik.ac.kr

Jawad Ahmad
jawad.saj@gmail.com

Arshad Ali
arshadali.giki@gmail.com

[1] Department of Electronics and Computer Engineering, Graduate School, Hongik University, Seoul, South Korea

[2] Department of Computer and Information Communication Engineering, Hongik University, Seoul, South Korea

[3] School of Engineering and Built Environment, Glasgow Caledonian University, Glasgow, Scotland, UK

1 Introduction

In the era of technology and development with the ever-growing advancement of both computer and Internet, multimedia data (audios, videos and images) is being extensively used in diverse applications, for example, military, E-commerce, Telemedicines, video conferencing, broadcasting and financial transaction, etc. Digital imaging applications are widespread and rapidly increasing day by day, yet the major hurdles in the expansion of applications and services are security, storage and confidentiality [1]. Since all the existing transmission mediums or networks which are either wired or wireless are insecure, transmitted data can be interrupted, intercepted and modified [2]. In such a scenario, a natural question about the security and confidentiality of multimedia data arises. The solution is provided by cryptography, the art of science which is currently considered as a branch of both computer science and mathematics, i.e., cryptography. Cryptography is defined as a science surrounding all the principle, rules, sets of instructions and methods for converting understandable and clear message into the form that is unintelligible and then reconverting that unintelligible message into original form [3]. To provide security, authenticity and confidentiality for multimedia data, two commonly known technologies are encryption and watermarking [4].

Encryption is defined as the process of translating plaintext message into a form known as ciphertext message. This ciphertext message should not be read by anyone without a process known as decryption. Decryption is a reverse process of encryption which transforms the ciphertext back into the plaintext. Encryption is a process of applying special mathematical algorithms (set of rules) and keys to convert the original message into ciphertext while decryption involves the use of algorithms to obtain the original message back. Digital watermarking [5] is used to hide or embed information in multimedia data, so that the information becomes protected from illegal copying, manipulation and modification.

Watermark is classified on the basis of its application as visible or invisible watermark [6]. A visible watermark is typically embedded in digital image which consists of a clear visible message or a company logo indicating the ownership of the image. For example, in most of the currency bills, a visible watermark is typically embedded to distinguish bogus and genuine currency. In invisible digital watermarking, a signal is added in multimedia data such that it cannot be perceived [7, 8]. A digital watermarking scheme can be divided into two main areas: symmetric and asymmetric. In symmetric watermarking, keys are symmetric or identical during watermark embedding and detection process. If keys for watermark embedding and detection are different, then this type of watermarking is called the asymmetric watermarking [9–12].

An encryption algorithm can be divided into two types, block cipher and stream cipher. A block cipher is a type of encryption algorithm in which a block of plaintext is treated as a whole, and the output produced is a ciphertext block, where the block lengths of plaintext and ciphertext are the same. A block cipher encryption algorithm, for example, can take a 128-bit block of plaintext as input, and output a corresponding 128-bit block of ciphertext. Basically block cipher is a symmetric key cipher, which means that all blocks are encrypted and decrypted with the same key. For greater security, block length and key size are kept larger. A stream cipher is a type of encryption algorithm in which a digital data stream is encrypted one bit or one byte at a time. Examples of classical stream ciphers are the autokeyed Vigenre cipher and the Vernam cipher [13]. The basic purpose of using a stream cipher is to design algorithms which are exceptionally faster than a typical block

cipher. Stream ciphers are often used in order to lower hardware complexity and to execute at a higher speed than block ciphers [14]. Block ciphers have the advantage over the stream ciphers that a large block can be divided into a number of small blocks which can be serially encrypted [15].

There are many types of encryption algorithms depending upon the applications and requirements. One classification on the basis of volume of data to be encrypted is complete vs selective encryptions [5]. As their names indicate, in complete encryption, the whole data is encrypted, whereas in selective one, only a portion of the content is encrypted. Both of them have their own pros and cons. On the basis of security, complete encryption has higher security level because the whole multimedia data is transformed into unreadable form. In selective encryption algorithms, since only a portion of multimedia content is

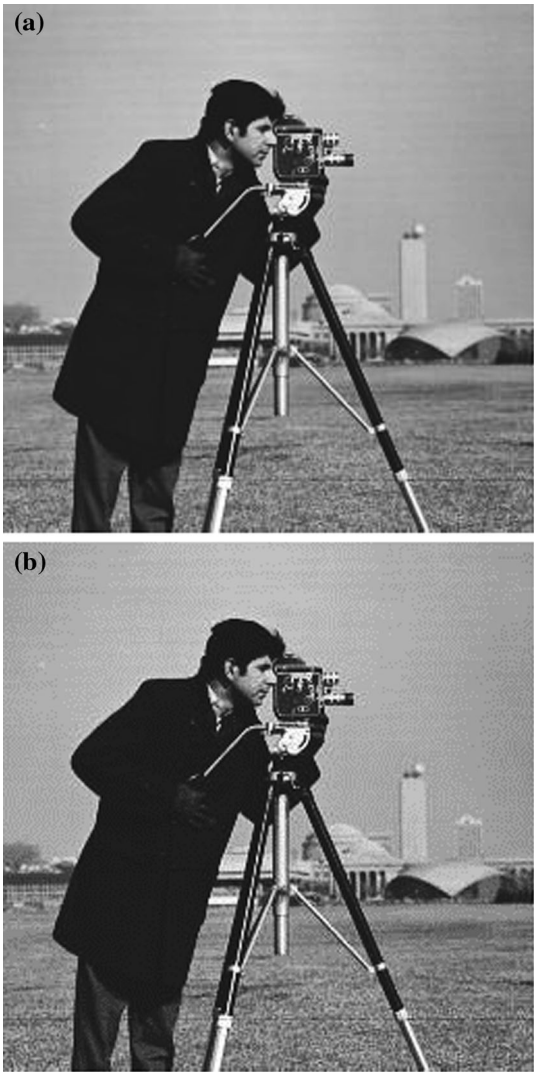

Fig. 1 Illustration of manipulation in an image. **a** Original Cameraman image. **b** Compressed version of the image shown in Fig. 1.1a, JPEG QF = 70

encrypted, security level declines accordingly. Complete encryption has low efficiency due to the large size of data to encrypt, while in selective encryption, less time is required for encryption/decryption, resulting in high efficiency of algorithms. Complete encryption is also known as direct encryption and selective encryption as partial encryption [13, 16].

Encryption algorithms can be classified into two major types, symmetric and asymmetric key algorithms [13, 16]. In symmetric key algorithm, the same key is used for encryption and decryption. That is why it is also known as private key algorithm or one-key encryption [13, 16]. DES (Data Encryption Standard), 3DES (Triple DES), AES (Advanced Encryption Standard), CFES (Compression Friendly Encryption Standard) and CCCMES (Chaotically Coupled Chaotic Map Encryption Scheme) are the examples of symmetric key algorithms. Asymmetric key algorithm, also known as public key algorithm [13, 16], makes use of two different keys for encryption and decryption of the message, respectively. These two keys are called the public key and the private key. To encrypt an original message, public key is used and for decryption, private key is used. RSA is the most common example of asymmetric key algorithm. Symmetric key algorithm has an advantage of high speed over asymmetric one. In asymmetric key cryptography, speeds of encryption and decryption are slow and it is considered appropriate for short messages such as keys.

A common question which arises is that when the field of cryptography is already well matured, why are new image encryption techniques required [17]? Traditional cryptographic techniques, like block cipher, change in a single bit of the encrypted image can cause a complete decryption failure. This is because traditional cryptographic techniques have been designed for text-based applications where each bit should be correctly decrypted to ensure the successful decipherment of the transmitted message. The situation is a bit different in multimedia applications like images. What matters in digital images is the content of an image rather than the exact pixels values. For example, Fig. 1a, b show an original and its JPEG compressed Cameraman images, respectively. Although both images are perceptually the same, however, the pixels values are different. Lossy compression, enhancement and geometric transformation are common operations for digital images. If an image is encrypted using a traditional encryption scheme like AES, and then passed through JPEG lossy compression, the decryption will totally fail. In conventional cryptographic techniques the decrypted data is exactly the same as the original or plaintext data. However, this is not necessary requirement for multimedia data that involves audio, image or video. As discussed above, in most of the multimedia applications, an approximation of the original multimedia content is sufficient and small distortion is acceptable due to human visual perception [17].

Recently, as exchange of multimedia data has dramatically increased over the Internet, security issues of multimedia are also emerged. This has motivated researchers to develop novel multimedia encryption schemes [12, 13, 16]. Although these encryption schemes meet various application requirements, they are still not mature. One aspect that needs attention is the security analysis of the schemes proposed in the literature. A number of encryption schemes have been found to be insecure [2, 12, 18, 19]. This provides the basic motivation behind this research. Multimedia encryption and decryption schemes should be designed in such a way that it encompasses a high level of security and efficiency [19]. In image encryption algorithms, the most important issue is how to determine the quality of encryption in terms of security and efficiency [20]. The main theme of this paper is to investigate the security and efficiency of some traditional image encryption schemes. As such, there is a real need to develop techniques that can address the challenges in

multimedia content and services. A general framework presented in [1] is used for the evaluation of image encryption schemes.

The quality of an image encryption scheme can be judged by visual inspection, but in some cases it may not give any indication about the hidden loopholes. In this research, the primary objective is to study a number of parameters that help to evaluate an image encryption scheme. Using these parameters, a comparison of conventional encryption schemes like Advanced Encryption Standard (AES), Compression Friendly Encryption Scheme (CFES) [17], Chaotically Coupled Chaotic Map Encryption Scheme (CCCMES) [21] and Bernoulli Map Based Encryption Scheme (BMBES) [22] is made to demonstrate the effectiveness of these schemes.

The rest of paper is organized as follows. Section 2 discusses the well known AES algorithm, CFES [17], CCCMES [21] and BMBES [22]. As visual inspection is not sufficient to judge the amount of features hidden in an encryption scheme, Sect. 3 discusses parameters to evaluate an image encryption scheme. Using these security parameters, a comparison study is also carried out among AES, CFES, CCCMES and BMBES. All the schemes were analyzed using parameters like correlation coefficient, information entropy, compression friendliness, Mean Square Error (MSE), Number of Pixel Change Rate (NPCR), Unified Average Change Intensity (UACI) and key sensitivity. The paper ends with conclusion in Sect. 4.

2 Overview of AES, CFES, CCCMES and BMBES

In this section, an overview of four traditional schemes (AES, CFES, CCCMES and BMBES) is discussed. Both AES and CFES are non-chaotic schemes, while CCCMES and BMBES are chaos-based image encryption schemes. For better understanding of security features, we briefly explain some fundamental knowledge of these schemes.

2.1 Overview of Advanced Encryption Standard

AES is the abbreviation of Advanced Encryption Standard adopted by the US government [23]. AES algorithm is a symmetric block cipher and used for electronic data encryption [13, 16]. AES was published by NIST (National Institute of Standard and Technology) in November 2001 and supersedes DES (Data Encryption Standard). In 1970, DES was designed and used for hardware implementation and does not produce efficient software code [13, 16, 19]. Then triple (3DES) was introduced to overcome the drawback of DES. 3DES has no cryptographic attack based on the algorithm itself except the brute force attack [13, 16, 19]. With respect to security, 3DES is very resistant against cryptanalysis. If security was the only concern, then 3DES is a strong candidate or an appropriate choice for a standard encryption algorithm. The major drawback with the 3DES is that it is very slow since it takes three times as many rounds as DES. DES and 3DES use a block size of 64 bits. For higher efficiency and security, larger block size is required. Due to the drawbacks of DES and 3DES, NIST issued a call for proposals in 1997 for a new encryption standard. NIST specified in its proposal that the new algorithm must be symmetric block cipher with block length of 128 bit and support key lengths of 128, 192 and 256 bits [13, 16, 19]. After the evaluation of several algorithms, NIST selected the Rijndeal algorithm as the de facto standard. Rijndeal's algorithm which is now known as Advanced Encryption Standard (AES) was developed by two Belgian

cryptographers, Joan Daemen and Vincent Rijmen. As compared to DES, AES has stronger security and improved efficiency. Interested readers can find technical details of AES in [23].

2.2 Compression Friendly Encryption Scheme

In the era of communication, all the encryption techniques faced the same problem of storage capabilities. Most commonly used encryption techniques such as DES (Data Encryption Standard), 3DES (triple Data Encryption Standard) and AES are not compression friendly, i.e., even a one bit change in the ciphertext will result in the complete failure of decryption process. So to overcome this major issue for the recovery of original information the authors in [17] proposed a new algorithm titled "Compression Friendly Encryption Scheme." The most distinguishing property of this technique is the capability to tolerate JPEG compression. This means that if the encrypted image is JPEG compressed, decryption is possible with some acceptable distortion.

In [17] the authors had designed an image encryption technique which not only fulfils the requirement of the cryptography but is also capable of withstanding the JPEG lossy compression. An important point to highlight here is that CFES is not proposed for lossless encryption. This encryption algorithm is capable of generating an image perceptually identical to the original plaintext with a high value of PSNR. To recover the original image with the exact value of pixels of image is not the part of CFES as in most of multimedia applications the image with reasonable perceptuality is acceptable rather than the exact pixel value of the recovered image. Depending on the requirements or applications, low level or high level encryption is achievable because it is capable of generating cipher images having variable perceptual distortions. The CFES encryption and decryption are shown in Fig. 2. Detail steps are given in [17].

2.3 Chaotically Coupled Chaotic Map Encryption Scheme

Chaotic systems have several significant features favourable to secure communication such as sensitivity to initial conditions, ergodicity, pseudo random property, deterministic, mixing (stretching and folding) and complexity. These are basically related to two important properties of cipher: confusion and diffusion mechanisms. Confusion mechanism rearranges the pixel values while diffusion mechanism changes the values of each pixel. Confusion and diffusion process can be repeated many times to obtain a higher security level [24]. Recently many different chaotic cryptosystems have been proposed. Security analysis of these new proposed chaotic cryptosystems needs a great attention. One example of chaotic base encrption scheme is proposed in [21]. The proposed encryption scheme in [21] is based on chaotically coupled chaotic maps. This scheme can be proved secure even with a single map due chaotic nature of maps. Chaotic discrete systems generate a periodic sequence, however, period increases exponentially with the number of coupled maps and hence maps are coupled for better security [21]. This cryptosystem utilizes only an essence of chaos: high sensitivity of the chaotic trajectory to initial conditions and reoccurrence property of chaotic trajectory. Authors [21] explore the parameters which only produce chaotic behaviour like chaotic

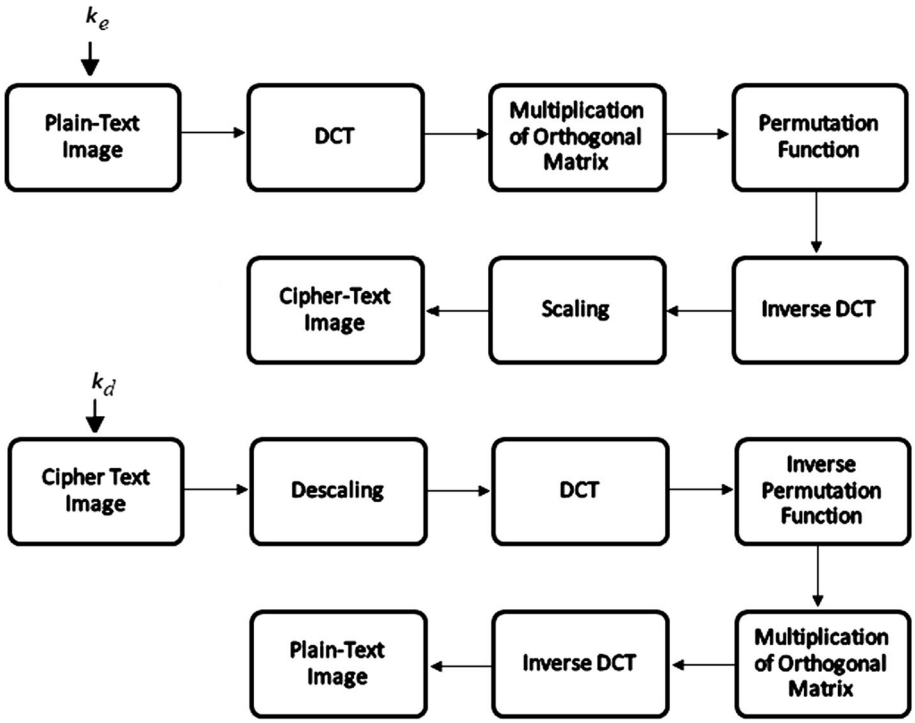

Fig. 2 Block diagram of CFES [17]

maps. A block diagram of CCCMES is shown in Fig. 3. Steps shown in Fig. 3 are discussed in more detail in [21].

2.4 Bernoulli Map Based Encryption Scheme

In [22], an efficient image encryption scheme based on generalized Bernoulli map is proposed. Both confusion and diffusion properties have been added in Bernoulli Map Based Encryption Scheme (BMBES). In confusion process, pixels positions are shuffled, while in diffusion, pixels values are modified by using generalized Bernoulli shift maps. First of all, pseudo-random numbers have been generated by utilizing Bernoulli shift maps. Permutation is carried out by using the methodology of sorting which is then applied on pseudo random numbers. To add diffusion characteristics in BMBES, two generalized Bernoulli shifts maps have been used to generate two pseudo-random grayscale value sequences. These new generated Pseudo- random numbers are utilized to modify the pixel gray values sequentially. This scheme is highly resistive to all known attacks because of sensitive initial conditions for generalized Bernoulli map. Encrypted image changes unpredictably even with one bit change in a plaintext image. Confusion and diffusion process of this scheme is shown in Figs. 4 and 5, respectively. Detail analysis of BMBES is discussed in [22].

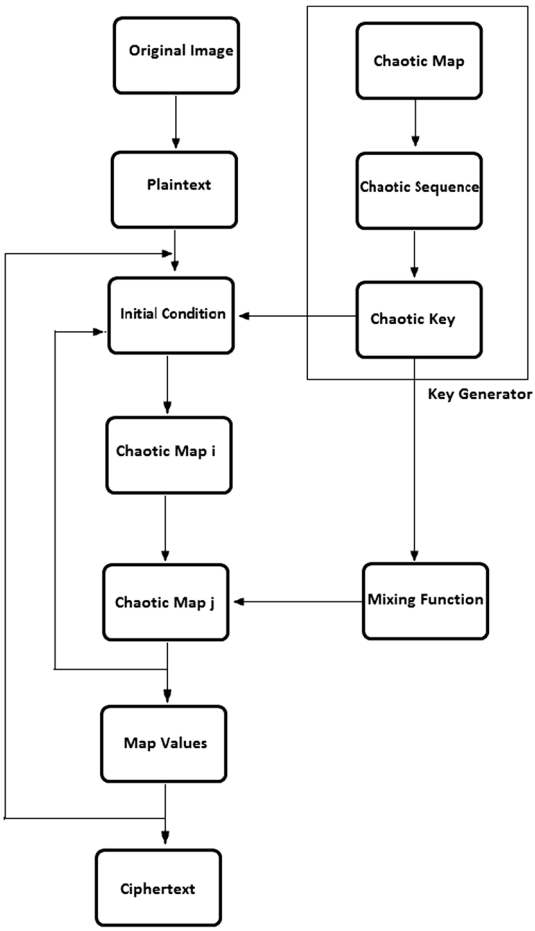

Fig. 3 Block diagram of CCCES [21]

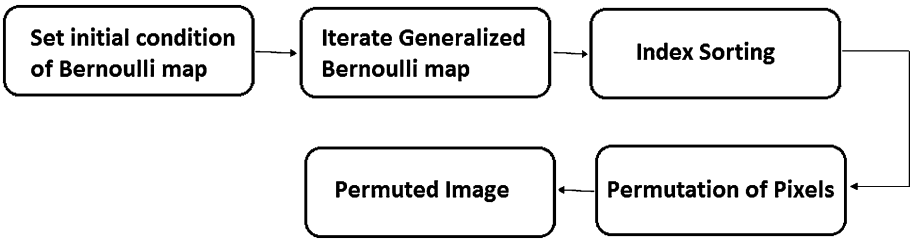

Fig. 4 Confusion process of BMBES

3 Experimental Results and Evaluations of AES, CFES, CCCMES & BMBES

This section discusses the security analysis of AES, CFES, CCCMES and BMBES. Comparison of these schemes is carried out using the security parameters like correlation coefficient, information entropy, compression friendliness, number of pixel change rate

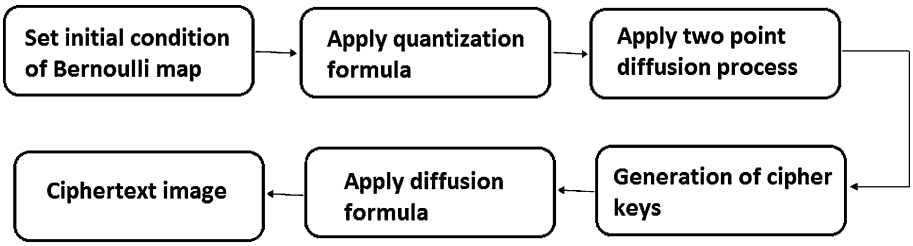

Fig. 5 Diffusion process of BMBES

and unified average change intensity, etc. Some interesting properties of these encryption schemes are presented in the subsequent sections.

3.1 Correlation Coefficient Analysis

Correlation coefficient is a statistical technique that measures the quality of encryption based on the linear relationship between two variables. In the case of image encryption, these variables are plaintext and ciphertext. Correlation coefficient shows the measure of dependence and strength between two quantities [33]. It takes on values ranging between $+1$ and -1. Zero correlation means that the correlation statistic did not indicate a relationship between the two variables. If the correlation coefficient is 1, it means that plaintext and ciphertext are highly dependent and there is a perfect correlation. In the case of perfect correlation, encrypted image is exactly the same as that of plaintext image. A negative correlation coefficient indicates a perfect negative linear relationship which means that encrypted image is negative of plaintext image. The smaller the value of correlation coefficient is, the better the quality of encryption is. Mathematically, correlation coefficient can written as [20, 25, 26]:

$$C \cdot C = \frac{Cov(x, y)}{\sigma_x \times \sigma_y}. \tag{1}$$

$$\sigma_x = \sqrt{VAR(x)}. \tag{2}$$

$$\sigma_y = \sqrt{VAR(y)}. \tag{3}$$

$$VAR(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2. \tag{4}$$

$$Cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{5}$$

where $C \cdot C$ is correlation coefficient and Cov is covariance at pixels x and y, x and y are the grayscale values of two pixels in the same place in the plaintext and ciphertext images. $VAR(x)$ is variance at pixel value x in the plaintext image, σ_x is standard deviation, E is the expected value operator and N is the total number of pixels for $N \times N$ matrix.

The well known Cameraman and Baboon images are used to test all encryption schemes for correlation coefficient analysis. Tests are performed by selecting 1000 pairs of adjacent

Table 1 Correlation coefficient of two adjacent pixels: Cameraman image

Direction of adjacent pixels	Plaintext Image	Ciphertext AES	Ciphertext CFES	Ciphertext CCCMES	Ciphertext BMBES
Horizontal	0.9282	−0.0067	0.9522	−0.0060	−0.0417
Vertical	0.9644	0.0504	0.0124	0.0507	0.0613
Diagonal	0.9116	−0.0156	0.0202	0.0148	0.0057

Table 2 Correlation coefficient of two adjacent pixels: Baboon image

Direction of adjacent pixels	Plaintext Image	Ciphertext AES	Ciphertext CFES	Ciphertext CCCMES	Ciphertext BMBES
Horizontal	0.7103	−0.037	0.9547	0.0273	−0.0170
Vertical	0.5966	0.0107	0.0611	0.0253	−0.0115
Diagonal	0.6225	−0.0419	−0.0025	0.0099	0.0095

pixels. Correlation coefficient between two horizontally adjacent pixels, two vertically adjacent pixels and two diagonally adjacent pixels, respectively, are performed. The simulation results are mentioned in Tables 1 and 2 for horizontally, vertically and diagonally adjacent pixels, respectively.

The tables show that the correlation for vertical and diagonal adjacent pixels is close to zero, i.e., minimum for all above mentioned encryption schemes. The correlation between the pixels of plaintext image is maximum, i.e., near to 1. Horizontal correlation of adjacent pixels is minimum, approximately close to zero for all schemes except CFES.

3.2 Entropy Analysis

Entropy is an important parameter for analyzing an encryption scheme. Entropy is related with the measure of information contained in the data and shows the degree of unpredictability and randomness in a system [36]. In a technical term, entropy measures the level of difficulty to predict a system. In this context, the term usually refers to the Shannon entropy which was introduced by Claude. E. Shannon in 1948. The quality of image encryption is usually determined by the Shannon entropy over the ciphertext image [27]. If an image is encrypted, it decreases the mutual information among pixel values and thus increases the entropy. Entropy of a message m can be represented as $H(m)$ for m symbols and $p(m_i)$, where $p(m_i)$ is the probability of occurrence of symbol m_i. A proper secure system should meet a condition on information entropy such that a ciphertext image should not provide any information about the original image [28]. The entropy $H(m)$ of any message can be calculated as [29–31]:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \times \log_2 \frac{1}{p(m_i)}, \tag{6}$$

Information entropy test has been performed for Cameraman and Baboon images of size 256×256. For these images, the theoretical value is 8 bits. If an encryption scheme has

Table 3 Entropy results

Encrypted image	AES	CFES	CCCMES	BMBES
Cameraman	7.9975	7.1455	7.9828	7.9973
Baboon	7.9973	7.1404	7.9881	7.9973

less value than 8, then this scheme will be insecure because of the possibility of predictability. Simulation results for all schemes are shown in Table 3. As from the table, it can be noticed that the entropy value of CFES is less than other three schemes. So it is easy to predict the original image in the case of CFES and hence CFES is insecure against entropy attack. The value for entropy is greater than 7.98 for AES, CCCMES and BMBES. The entropy analysis shows that security is high for all schemes except CFES.

3.3 Encryption Quality Measurement

An important issue in image encryption algorithms is the evaluation of the quality of encryption. Earlier studies on image encryption were based on visual inspection to judge the effectiveness of an encryption technique [20]. An image encryption algorithm is good, if it is able to conceal a large number of image features. In some scenarios, visual inspection is sufficient but it does not give an indication about the amount of information concealed. To judge the quality of encryption, a number of measuring techniques are proposed in the literature [18–20, 25, 32].

3.3.1 Maximum Deviation

The maximum deviation measures the quality of encryption scheme in the sense that how it maximizes the deviation between plaintext and ciphertext [33]. The More the ciphertext deviated from the plaintext, the better the encryption algorithm is. Steps for the calculation of maximum deviation are shown in [34].

3.3.2 Irregular Deviation

The irregular deviation measures how much the statistical distribution of histogram deviation is close to uniform distribution. If irregular deviation is close to uniform distribution then the encryption algorithm is said to be good [20]. The irregular deviation is calculated as follows:

1. Take the absolute difference of plaintext (P) and the ciphertext (C) image [20].

$$D = |P - C|, \tag{7}$$

2. Calculate the histogram of D.

$$H = histogram(D). \tag{8}$$

3. Let h_i be the amplitude of histogram at index i. Then the average value of M_H is:

$$M_H = \frac{1}{256}\sum_{i=0}^{255} h_i, \tag{9}$$

4. Calculate the absolute of the histogram deviations using M_H as follows [20]:

$$H_{D_i} = |h_i - M_H|. \tag{10}$$

5. Now irregular deviation I_D can be calculated [20]:

$$I_D = \sum_{i=0}^{255} H_{D_i}. \tag{11}$$

The smaller the value of I_D is, the better the encryption quality is.

3.3.3 Deviation From Uniform Histogram

Histogram shows the frequency distribution of pixels of an image. A histogram uses a bar graph in which the horizontal axis represents the gray level values and the vertical bar represents the corresponding number of gray levels [18]. The histogram associated to the encrypted image should hide the frequency distribution of original image. Using histogram, an attacker does frequency analysis to deduce the secret key known as statistical attack. To prevent statistical attack, the histogram of plaintext image and histogram of ciphertext image should not have any similarity. A ciphertext image should have uniform distribution for higher security. Relatively uniform distribution of the ciphertext image shows that encryption algorithm has a good quality. For an image encryption algorithm, the histogram of encrypted image possesses two important properties: (1) it should be totally different of the histogram of plaintext image; (2) it should have a uniform distribution which means that probability existence of each pixel value is the same and totally random. This can be formulated as [18]:

$$H_{C_i} = \begin{cases} \dfrac{M \times N}{256} & 0 \le C_i \le 255 \\ 0 & \text{elsewhere} \end{cases} \tag{12}$$

The deviation from uniform histogram shown by Eq. 12 is calculated as [18]:

$$D_p = \frac{\sum_{C_i=0}^{255} |H_{C_i} - H_C|}{M \times N}, \tag{13}$$

where H_C is the histogram of the encrypted image and H_{C_i} is ideally encrypted image which has a complete uniform histogram distribution. The lower the value of D_p is, the better encryption quality is.

The Cameraman and Baboon images are tested to evaluate maximum deviation (M_D), irregular deviation (I_D) and deviation from uniform histogram (D_p). Results for all schemes are shown in Tables 4 and 5. It can be observed that AES and BMBES have higher values of maximum deviation than CFES and CCCMES. Results of maximum

Table 4 Encryption quality results for Cameraman image

Encryption schemes	D	I_D	D_p
AES	6.1799×10^4	39,958	12.1406
CFES	5.6285×10^4	56,478	230.4063
CCCMES	5.5021×10^4	42,382	30.8906
BMBES	6.1730×10^4	39,702	12.8125

Table 5 Encryption quality results for Baboon image

Encryption schemes	D	I_D	D_p
AES	5.8929×10^4	51,848	14.0703
CFES	2.2393×10^4	77,670	158.2109
CCCMES	5.3112×10^4	51,894	26.5156
BMBES	5.8874×10^4	50,102	12.1953

deviation parameter highlights that AES and BMBES are more secure. CFES has a smaller value of maximum deviation and hence a lower level of information hiding. With respect to maximum deviation, AES can be a better candidate for encryption of data.

When the value of irregular deviation is less, the scheme is more secure. BMBES algorithm has a smaller value than all other three schemes. In terms of deviation , BMBES is better than all the other schemes because deviation of pixels values of plaintext and corresponding ciphertext is higher and random. In the case of (D_p) analysis, AES and BMBES have smaller values than CFES and CCCMES. The fact that both CFES and CCCMES have greater values indicates that ciphertext images are more deviated from their ideal histograms. One can say that, by the encryption quality measures, BMBES can be considered better as compared to AES, CFES and CCCMES.

3.4 Avalanche Effect

Avalanche effect is a desirable property for checking the efficiency of diffusion mechanism. A single bit change in a plaintext image P can cause a significant modification in its corresponding ciphertext image C. This effect is known as avalanche effect [35]. In block ciphers, a small change in key or plaintext should cause a drastic change in the ciphertext. Let C_1 and C_2 be two ciphertext images whose corresponding keys differ by one bit. The avalanche effect is the percentage of difference between C_1 and C_2. If C_1 and C_2 differ from each other in half of their bits, we can say that the encryption algorithm possesses good diffusion characteristics [36].

MSE can be calculated as [37, 38]:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [C_1(i,j) - C_2(i,j)]^2, \tag{14}$$

where M and N is the width and height of images and $C_1(i,j)$ is grayscale value of pixel at grid (i,j) in ciphertext image C_1 and $C_2(i,j)$ is grayscale value of pixel at grid (i,j) in ciphertext image C_2. In [39], authors discussed MSE and generally speaking, if value obtained using Eq. 14 is $\geq$30 dB, the difference between two images is evident [39]. From Table 6, it is clear that all encryption schemes have MSE values greater than 30. It can be seen from Table 6, that chaotic map based encryption schemes have greater value of MSE as compared to non-chaotic encryption schemes. This feature highlights an interesting property of chaos-based encryption scheme that by changing one bit in a plaintext image the difference between ciphertext images are evident. It is due to the fact that chaotic maps is more sensitive to the change in a plaintext image. From Table 6, it is clear that CFES is less sensitive to the change in the plaintext images.

Table 6 Mean square error (MSE) results

Encrypted image	AES (dB)	CFES (dB)	CCCMES (dB)	BMBES (dB)
Cameraman	40.3443	33.3118	40.7237	40.4947
Baboon	40.3650	33.6265	40.7875	40.5799

3.5 Number of Pixels Change Rate (NPCR) and Unified Average Change Intensity (UACI)

To test the sensitivity of single bit change on a whole encrypted image, two common measures are used: NPCR and UACI. NPCR and UACI are two most widely used security analysis for differential attacks. Number of Pixels Change Rate (NPCR) shows the percentage of different pixel numbers between two encrypted images whose plaintexts have a difference of only one pixel. Unified Average Change Intensity (UACI) shows the differences of average intensities between two ciphertext images whose corresponding plaintext have a difference of only one pixel [40].

Let C_1 and C_2 be two different ciphertext images whose corresponding plaintext images differ by only one bit. Label the grayscale value of the pixel at grid (i,j) in C_1 and C_2 by $C_1(i,j)$ and $C_2(i,j)$, respectively. We define an array D to have the same size as C_1 and C_2. Then $D(i,j)$ is determined by using $C_1(i,j)$ and $C_2(i,j)$ as: if $C_1(i,j) = C_2(i,j)$ then $D(i,j) = 0$, otherwise $D(i,j) = 1$.

The *NCPR* is defined as [15, 41]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\,\%, \tag{15}$$

where W and H are the width and height of ciphertext images C_1 and C_2, respectively.

By using Eq. 15, the percentage of different pixel numbers between the plaintext image and the ciphertext image can be calculated. *NCPR* can also be defined as the variance rate of pixels in the encrypted image caused by the change of a single pixel in the original image [30].

Unified Average Change Intensity $(UACI)$ determines the average intensity of differences between two images. Mathematically, *UACI* can be defined as [37, 38]:

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\,\%. \tag{16}$$

The higher the value of *NPCR* and *UACI* is, the better the quality of encryption is. From Tables 7 and 8, it is clear that CCCMES has good diffusion characteristics than AES, CFES and BMBES. With respect to NPCR and UACI, the results in Tables 7 and 8 show that CFES has less sensitivity to small changes in plaintext images. Generally, these results reflect that CCCMES has strong diffusion mechanism as compared to other schemes.

3.6 Key Sensitivity Test

A good encryption algorithm should be sensitive to secret key and plaintext, i.e., the change of single bit in the secret key or plaintext should cause a drastic change in the

Table 7 Number of pixel change rate (NPCR) results

Images	AES	CFES	CCCMES	BMBES
Cameraman	99.6167	99.0341	99.6805	92.2653
Baboon	99.6078	99.1898	99.6323	99.2299

Table 8 Unified average change intensity (UACI) results

Images	AES	CFES	CCCMES	BMBES
Cameraman	33.4040	14.4458	34.9374	30.9867
Baboon	33.5018	15.0174	35.6980	33.3377

Table 9 Difference of two ciphers when keys differ by one bit

Images	AES (%)	CFES (%)	CCCMES (%)	BMBES (%)
Cameraman	99.5880	99.2554	99.5988	99.6002
Baboon	99.5728	99.1379	99.6231	99.6246

ciphertext [13]. Secure cryptosystems require high key sensitivity, which means that encrypted image should not be decrypted correctly even if there is only a small difference between encryption and decryption keys. Let C_1 and C_2 be two different ciphertext images whose corresponding keys differ by only one bit. The percentage difference between two ciphertext images are calculated, whose corresponding keys differ by one bit only. Simulation results are depicted in Table 9, which shows that all encryption schemes have good results for key sensitivity. By changing just one bit in the key, more than 99 % changes occur in encrypted images. The schemes based on chaotic maps have better results than non-chaotic maps.

4 Conclusion

In this paper, four techniques have been presented for security evaluation. Results have been carried out to analyze which technique is better to transmit multimedia data over a medium more securely. Comparison analysis was done on the basis of security parameters like correlation coefficient, information entropy analysis, encryption quality, NPCR, UACI, MSE and key sensitivity test.

In correlation coefficient analysis, results show that correlation for vertical and diagonal adjacent pixels is close to zero, i.e., minimum as needed for all schemes. Except CFES, correlation of horizontal adjacent pixels is also minimum for all schemes. Less correlation values of an encrypted image indicates higher security. Entropy values for CFES were less as compared to AES, CCCMES and BMBES. All three schemes having higher entropy values are more secure and possess resistive properties against entropy attacks. Maximum deviations of AES and BMBES have higher values as compared to other two schemes. AES and BMBES are very secure with respect to maximum deviation parameter. The values of irregular deviation parameter are less for CCCMES which indicates that it is better than AES, CFES and BMBES. BMBES has smaller value

for deviation from uniform histogram. In the case of BMBES, the lower value of deviation from uniform histogram represents better encryption quality because the lower value points out that the histogram of cipertext image is less deviated from uniform histogram.

Diffusion characteristic of cryptosystem is an important parameter for comparison of different encryption schemes. For this purpose, avalanche effect test is performed in terms of NPCR, UACI and MSE, respectively. From results obtained through NPCR, UACI and MSE, we observed that all encryption schemes show significant differences for small changes, i.e., they all have values of MSE >30 dB. As compared to other schemes, CCCMES has higher values of MSE, NPCR and UACI. The values of MSE for CFES are approximately 34 dB which means that by changing one bit in plaintext, the difference between ciphertext images is not high. The key sensitivity test points out that more than 99% changes occurs for different keys in all schemes.

Acknowledgments It was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2014R1A1A2054174) and the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the Global IT Talent support program (NIPA-2014-H0905-14-1004) supervised by the NIPA (National IT Industry Promotion Agency).

References

1. Ahmad, J., & Ahmed, F. (2012). Efficiency analysis and security evaluation of image encryption schemes. *International Journal of Video & Image Processing and Network Security*, *12*(04), 18–31. ISSN: 2077–1207.
2. Jakimoski, G., & Subbalakshmi, K. (2008). Cryptanalysis of some multimedia encryption schemes. *Multimedia, IEEE Transactions on*, *10*(3), 330–338.
3. Acharya, B., Patra, S., & Panda, G. (2008). Image encryption by novel cryptosystem using matrix transformation. In *Emerging trends in engineering and technology, 2008. ICETET'08. First international conference on* (pp. 77–81), IEEE.
4. Furht, B., & Socek, D. (2003). A survey of multimedia security. *Comprehensive report on*.
5. Lian, S., Liu, Z., Ren, Z., & Wang, H. (2006). Secure advanced video coding based on selective encryption algorithms. *Consumer Electronics, IEEE Transactions on*, *52*(2), 621–629.
6. Mohanty, S.P., Ramakrishnan, K., & Kankanhalli, M. (1999). A dual watermarking technique for images. In *Proceedings of the seventh ACM international conference on Multimedia (Part 2)* (pp. 49–51). ACM.
7. Hartung, F., & Girod, B. (1998). Watermarking of uncompressed and compressed video. *Signal processing*, *66*(3), 283–301.
8. Hartung, F., & Girod, B. (1996). Digital watermarking of raw and compressed video. In *Proceedings of European EOS/SPIE Symposium on Advanced Imaging and Network Technologies* vol. 2952, (pp. 205–213). Citeseer.
9. Van De Ville, D., Philips, W., Van de Walle, R., & Lemahieu, I. (2004). Image scrambling without bandwidth expansion. *Circuits and Systems for Video Technology, IEEE Transactions on*, *14*(6), 892–897.
10. Chen, Y., & Chang, L. (2001). A secure and robust digital watermarking technique by the block cipher rc6 and secure hash algorithm. In *Image processing, 2001. Proceedings. 2001 international conference on* vol. 2, (pp. 518–521). IEEE.
11. Chandramouli, R., Memon, N., & Rabbani, M. (2002). Digital watermarking. *Encyclopedia of Imaging Science and Technology*.
12. Furht, B., & Kirovski, D. (2005). *Multimedia security handbook* (Vol. 4). Boca Raton: CRC.
13. Stallings, W. (2010). *Cryptography and network security: Principles and practice* (Vol. 998). New Jersey: Prentice Hall.
14. Abdul, D., Elminaam, H., & Hadhoud, M. Performance evaluation of symmetric encryption algorithms. *Communications, 8*.
15. Mao, Y., & Chen, G. (2005). Chaos-based image encryption. *Handbook of Geometric Computing* (pp. 231–265).

16. Schneier, B. (1996). *Applied cryptography*. USA: Wiley.
17. Ahmed, F., Siyal, M., & Abbas, V. (2010). A perceptually scalable and jpeg compression tolerant image encryption scheme. In *Image and video technology (PSIVT), 2010 Fourth Pacific-Rim Symposium on* (pp. 232–238). IEEE.
18. Elashry, I. E. (2010). *Digital image encryption*. MS Thesis, Department of Computer Science and Engineering, Faculty of Electronic Engineering Menofia University.
19. Lian, S. (2008). *Multimedia content encryption: Techniques and applications*. Boca Raton: Auerbach Publications.
20. Elkamchouchi, H., & Makar, M. (2005). Measuring encryption quality for bitmap images encrypted with rijndael and kamkar block ciphers. In *Radio science conference, 2005. NRSC 2005. Proceedings of the twenty-second national* (pp. 277–284). IEEE.
21. Pisarchik, A., & Zanin, M. (2008). Image encryption with chaotically coupled chaotic maps. *Physica D: Nonlinear Phenomena*, *237*(20), 2638–2648.
22. Ye, R. (2011). An image encryption scheme with efficient permutation and diffusion processes. In *Advances in computer science and education applications* (pp. 32–39). Springer.
23. Aes, N. (2001). Advanced encryption standard. *Federal Information Processing Standard, FIPS-197*, vol. 12.
24. Wong, K.-W. (2002). A fast chaotic cryptographic scheme with dynamic look-up table. *Physics Letters A*, *298*(4), 238–242.
25. El-Fishawy, N., & Zaid, O. (2007). Quality of encryption measurement of bitmap images with rc6, mrc6, and rijndael block cipher algorithms. *International Journal of Network Security*, *5*(3), 241–251.
26. Kamali, S., Shakerian, R., Hedayati, M., & Rahmani, M. (2010). A new modified version of advanced encryption standard based algorithm for image encryption. In *Electronics and Information Engineering (ICEIE), 2010 International Conference On* vol. 1, (pp. V1–141). IEEE.
27. Carter, T. (2007). *An introduction to information theory and entropy*. Santa Fe: Complex Systems Summer School.
28. Liang, J., & Shi, Z. (2004). The information entropy, rough entropy and knowledge granulation in rough set theory. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *12*(01), 37–46.
29. Ahmed, H., Kalash, H., & Allah, O. Implementation of rc5 block cipher algorithm for image cryptosystems. *International Journal of Information Technology 3*(4)
30. Enayatifar, R. (2011). Image encryption via logistic map function and heap tree. *International Journal of Physcical Science*, *6*(2), 221.
31. Han, Z., Feng, W., Hui, L., Da Hai, L., & Chou, L. (2003). A new image encryption algorithm based on chaos system. In *Robotics, intelligent systems and signal processing, 2003. Proceedings. 2003 IEEE international conference on*, vol. 2, (pp. 778–782). IEEE.
32. Ahmed, H., Kalash, H., & Allah, O. (2007). Encryption efficiency analysis and security evaluation of rc6 block cipher for digital images. In *Electrical engineering, 2007. ICEE'07. International conference on* (pp. 1–7). IEEE.
33. Dhawan, S. (2011). A review of image compression and comparison of its algorithms. *International Journal of electronics & Communication technology*, *2*(1).
34. Li, S., Chen, G., & Zheng, X. (2006). Chaos-based encryption for digital image and video. *Multimedia Encryption and Authentication Techniques and Applications* (p. 129).
35. Kumar, A., & Tiwari, M. N. (2012). Effective implementation and avalanche effect of aes. *International Journal of Security, Privacy and Trust Management (IJSPTM)*, *1*(3/4), 31–35.
36. El-Wahed, M.A., Mesbah, S., & Shoukry, A. (2008). Efficiency and security of some image encryption algorithms. In *Proceedings of the world congress on engineering* vol. 1, (pp. 2–4). London.
37. Mohamed, A., Zaibi, G., & Kachouri, A. (2011). Implementation of rc5 and rc6 block ciphers on digital images. In *Systems, signals and devices (SSD), 2011 8th international multi-conference on* (pp. 1–6). IEEE.
38. Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2008). Securing information content using new encryption method and steganography. In *Digital information management, 2008. ICDIM 2008. Third international conference on* (pp. 563–568), IEEE.
39. Liehuang, Z., Wenzhuo, L., Lejian, L., & Hong, L. (2006). A novel image scrambling algorithm for digital watermarking based on chaotic sequences. *International Journal of Computer Science and Network Security*, *6*(8B), 125–130.
40. Sethi, N., & Sharma, D. (2012). A novel method of image encryption using logistic mapping. *International Journal of Computer Science Engineering*, *1*(2), 115–119.

41. Nien, H., Changchien, S., Wu, S., & Huang, C. (2008). A new pixel-chaotic-shuffle method for image encryption. In *Control, automation, robotics and vision, 2008. ICARCV 2008. 10th International conference on* (pp. 883–887). IEEE.

Jawad Ahmad received his B.S. degree in Electronics Engineering in 2009 form Muhammad Ali Jinnah University, Pakistan and his M.S. degree in Electrical Engineering technology, from HITEC University, Pakistan, in 2012. Currently, he is a Ph.D. candidate in the Department of Electronics and Computer Engineering, Hongik University, South Korea. His interest includes nonlinear dynamics, cryptography, secure communications and image encryption.

Seong Oun Hwang received his B.S. degree in mathematics in 1993 from Seoul National University, his M.S. degree in computer and communications engineering in 1998 from Pohang University of Science and Technology, and his Ph.D. degree in computer science from Korea Advanced Institute of Science and Technology. He worked as a software engineer at LG-CNS Systems, Inc. from 1994 to 1996. He worked as a senior researcher at Electronics and Telecommunications Research Institute (ETRI) from 1998 to 2007. Since 2008, he has been working as associate professor with the Department of Computer and Information Communication Engineering of Hongik University, Korea. His research interests include cryptography including image encryption and cyber security.

Arshad Ali received his B.S. degree in Electronic Engineering from Ghulam Ishaq Khan Institute of Engineering Sciences and Technology (Pakistan) in 2011. He obtained Master degree from University of Strathclyde Glasgow in 2011 and currently working towards Ph.D. in Glasgow Caledonina University, Scotland, United Kingdom. Before this he worked as a lecturer in HITEC University Pakistan for 1 year. His main research interests include, chiral medium, image processing, and high voltage engineering.