Abstract—In recent years, there has been significant development in multimedia technologies. Transmission of multimedia data such as audio, video and images over the Internet is now very common. The Internet, however, is a very insecure channel and this poses a number of security issues. To achieve confidentiality and security of multimedia data over an insecure channel like the Internet, a number of encryption schemes have been proposed. The need to develop new encryption schemes comes from the fact that traditional encryption schemes for textual data are not suitable for multimedia data stream. This paper presents a framework to evaluate image encryption schemes proposed in the literature. Instead of visual inspection, a number of parameters, for example, correlation coefficient, information entropy, compression friendliness, number of pixel change rate and unified average change intensity etc., are used, to quantify the quality of encrypted images. Encryption efficiency analysis and security evaluation of some conventional schemes like the Advanced Encryption Standard (AES) and Compression Friendly Encryption Scheme (CFES) is also presented. The security estimations of AES and CFES for digital images against brute-force, statistical, and differential attacks are explored. Experiments results are presented to test the security of these algorithms for digital images. After analysis of AES and CFES, some weaknesses have been discovered in CFES. These weaknesses were mainly related to low entropy and horizontal correlation in encrypted images.

Index Terms—Image encryption, AES, encryption efficiency, compression friendly.

I. INTRODUCTION

Processing and transmission of multimedia contents over insecure networks, possesses several security problems. As a result, multimedia data security has become a serious and major issue in telemedicine, military, E-Commerce, financial transaction and mobile phone applications [1], [2]. To provide security attributes to multimedia contents, one needs to protect communicated information (plaintext) from unauthorized users. Multimedia contents needs to be secured from different types of attacks; for example, interruption, interception, modification and fabrication [3], [4]. Cryptography is basically scrambling of data for ensuring secrecy and/or authenticity of information. Cryptography enables us to transmit data across insecure networks so that it cannot be read by anyone except the authorized recipient. Cryptology and cryptanalysis are two main branches of cryptography. Cryptology is to keep plaintext secret from eavesdropper or simply the enemy while cryptanalysis deals with the defeating such techniques to recover information or forging information.

that will be accepted as authentic [4]. For secure transmission of multimedia data, information should be concealed from adversaries or attackers. Information is an asset like other assets [1]. So as an asset, information is to be kept secret from intruders, interceptor, attackers or simply the enemy [1]. Over global communication channels, people send sensitive personal information, corporate documents and financial transactions. In such scenarios; security, integrity, authenticity and confidentiality of digital data should be provided [5].

For security of multimedia data, two major technologies have been developed; encryption and digital watermarking. Encryption is the process of disguising a message [3]. In encryption, the content of multimedia data is protected and a key is required for proper decryption. The encrypted message is called the ciphertext and unencrypted message is called the plaintext. Obtaining the plaintext back from the ciphertext is known as decryption [3]. There are two types of algorithms used for encryption; symmetric-key algorithms and public-key algorithms [3], [4]. In most of the symmetric algorithms, the encryption key and the decryption key are same [3], [4]. In public key algorithms, encryption and decryption keys are different [3], [4]. The encryption key is made public so that any one can encrypt a message, however, only the person who has the correct private key can decrypt the message. It is believed that in a reasonable amount of time, it is infeasible to calculate the decryption key from the encryption key [3].

Digital watermarking is the process of embedding information into digital multimedia content such that the information can be protected from illegal copying and manipulation. A digital watermark is a signal added to a digital data, which can be extracted or detected later for a variety of purposes including copy prevention, control and authentication. [6]–[8]. Depending on the application, a watermark can be either visible or invisible [9]. 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 as video, audio, or an image such that it cannot be perceived [10], [11]. A digital watermarking scheme can 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 known as asymmetric [6]–[8], [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 length of plaintext and ciphertext is same. For example, a block cipher encryption algorithm might 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 is 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 Vigenere cipher and the Vernam cipher [4]. 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 due to lower hardware complexity and execute at a higher speed than block ciphers [13]. Block ciphers have the advantage over the stream ciphers that a large block can be divided into a number of small blocks and then the blocks can be serially encrypted [14].

In order to provide security and confidentiality, encryption algorithm can be classified into complete (direct) encryption and selective (partial) encryption [15]. In complete encryption, all multimedia content is encrypted [16]. It enables to encrypt large data volumes and hence has lower efficiency, but possesses higher security. In selective (partial) encryption, only a part of multimedia content is encrypted. Partial encryption algorithms reduces encryption and decryption time because encryption operation is implemented on small volume of data and thus has higher efficiency but at the same time has lower security [17]–[19]. Several researchers have combined encryption and compression into a single scheme. In such schemes, encryption and compression is implemented simultaneously [20], [21].

An image is a two-dimensional vector array. For image encryption, two dimensional data can be treated as one-dimensional textual bit stream, and any conventional cryptographic technique can be used. Direct encryption of multimedia data using traditional cryptographic technique is called naive encryption [5], [22]. Direct use of traditional cryptographic techniques for multimedia data has some limitations. Images are different from text, and hence the encryption of multimedia data is different due to some intrinsic features of images; for example bulk data capacity, high redundancy, strong correlation among pixels [23]–[25]. Processing time for encryption and decryption is also an important issue in real-time multimedia application. Traditional encryption schemes generally requires long computational time and high computing power [23]–[25].

A natural question which arises is that when the field of cryptography is already well matured, why new image encryption techniques are required [26]? In traditional cryptographic techniques, like block cipher, change in a single bit of the encrypted image can cause a complete decryption failure. Traditional cryptography techniques are designed for text-based applications in which each bit is required to be recovered correctly to clearly decipher the transmitted message. The situation is a bit different in multimedia applications, like images. In digital images the content of an image is what matters rather than the exact pixels values. Lossy compression, enhancement and geometric transformation are common operations for digital images. If an image is encrypted using a traditional encryption scheme like the AES, and then passed through JPEG lossy compression, the decryption will totally fail. In conventional cryptographic techniques, the decrypted data is exactly same as original or plaintext data. However, this requirement is not necessary 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 [26].

The rest of the paper is organized as follows. Section II, discusses parameters to evaluate an image encryption scheme. In Section III, a comparison study is carried out between the AES and CFES [26]. Both the schemes were analyzed using parameters like, correlation coefficient, information entropy, compression friendliness, Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI) etc. Section IV, discusses the modified CFES algorithm. Visual inspection is first carried out to judge the effectiveness of the modified cryptosystem. Then, by using several evaluation parameters, the quality of the modified scheme is studied. The paper ends with conclusion and presented in Section V.

II. PARAMETERS FOR THE EVALUATION OF AN IMAGE ENCRYPTION SCHEME

In this section, a number of parameters have been discussed. Using these parameters the efficiency and security of an image encryption scheme can be evaluated.

A. Correlation Coefficient

Correlation determines the relationship between two variables. In other words, correlation is a measure that computes degree of similarity between two variables. Correlation coefficient is a useful measure to judge encryption quality of any cryptosystem [27]. Any image cryptosystem is said to be good, if encryption algorithm hides all attributes of a plaintext image, and encrypted image is totally random and highly uncorrelated [27]–[29]. If encrypted image and plaintext image are completely different then their corresponding correlation coefficient must be very low, or very close to zero. If correlation coefficient is equal to one, then two images are identical and they are in perfect correlation. In case of perfect correlation (correlation coefficient is equal to 1), encryption process completely fails because the encrypted image is same as the plaintext image. When correlation coefficient is -1 then encrypted image is negative of original (plaintext) image.

In short, correlation coefficient between an image and itself is 1, correlation coefficient between an image and totally uncorrelated image is zero, and correlation coefficient between an image and its negative is -1 [28]–[30].

Let \( x \) and \( y \) be the gray-scale values of two pixels in the same place in the plaintext and ciphertext images. Then mathematically correlation coefficient can written as [28]–[30]:

\[
C.C. = \frac{Cov(x,y)}{\sigma_x \times \sigma_y}.
\]
\[ \sigma_x = \sqrt{VAR(x)}. \quad (2) \]
\[ \sigma_y = \sqrt{VAR(y)}. \quad (3) \]
\[ VAR(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2. \quad (4) \]
\[ Cov(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \quad (5) \]

where \( C.C \) is correlation coefficient and \( Cov \) is covariance at pixels \( x \) and \( y \), where \( x \) and \( y \) are the gray-scale 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, \( \sigma_x \) is standard deviation, \( E \) is the expected value operator and \( N \) is the total number of pixels for \( N \times N \) matrix.

### B. Information Entropy Analysis

Entropy of a source gives idea about self information i.e., information provided by a random process about itself [31]. The concept of entropy is very important for analyzing an encryption scheme. Information entropy is the main feature of uncertainty. It shows the degree of uncertainties in any communication system [32]. In 1949, Claude Elwood Shannon proposed that information theory is a mathematical theory of data communications and storage [33]. Nowadays, information theory is concerned with cryptography, network security, communication systems, data compression, error correlation and other related topics [34]–[36]. The entropy, \( H(m) \) of any message can be calculated as [34]–[36]:

\[ H(m) = \sum_{i=0}^{2^{N-1}} p(m_i) \times \log_2 \frac{1}{p(m_i)}. \quad (6) \]

where \( p(m_i) \) represent the probability of occurrence of the symbol \( m_i \).

Let us consider a true random source that generates \( 2^8 \) symbols with equal probability i.e., \( m = \{m_1...m_{256}\} \), where each symbol is represented by 8 bits. If Eq. 6 is evaluated for the aforementioned case, its entropy obtained is \( H(m) = 8 \) bits, which corresponds to a uniform random source. In general, the entropy value of the source is smaller than the ideal value, due to the fact that a real information source rarely transmits random messages. However, when messages are encrypted for a source that generates \( 2^8 \) symbols with equal probability, its entropy should be 8 bits ideally. In case if entropy is less than 8 bits, then there exists a certain degree of predictability [34], [35]. For a cryptosystem to resist the entropy attacks, the entropy of the cryptosystem should be close to ideal value [34]–[36].

### C. Compression Friendliness

There are some basic requirements of multimedia encryption that covers various aspects, including security, compression efficiency, encryption efficiency, and format compliance [18], [37]. The topic of multimedia compression has a vital role in the field of cryptography, since compression reduces storage space and transmission bandwidth. Based on the entropy theory, various compression coding methods have been introduced, such as, arithmetic coding, run length coding and LZW coding [18]. An encryption algorithm is compression friendly if it has small impact on data compression efficiency [37]. Some image encryption algorithms impact data compressibility or introduce additional data that is necessary for decryption process [18], [37].

Multimedia data has a lot of redundancy which can be compressed by entropy based coding methods. Multimedia data compression is an important step in encryption process which is applied before encryption, after encryption or during encryption [18]. However, in all cases, a small size of encrypted data is desirable.

### D. Encryption Quality

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 [30]. 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], [24], [28], [30], [38].

Deviation in pixel values between original image and encrypted image is a good parameter to express the quality of encryption [24], [30]. Randomness introduce in the encrypted image helps to conceal the features of plaintext image. The encryption quality is good, if deviation (changes) of pixels is maximum and irregular between the plaintext image and encrypted image. With the above discussion it is clear that deviation (change in pixel values) can be taken as a parameter to evaluate the quality of an image encryption scheme.

1) **Maximum Deviation:** By measuring the maximum deviation between the plaintext image and the corresponding encrypted image, the quality of encryption can be accessed [28]. The maximum deviation is calculated as follows [28]:

1. Calculate the histogram of the plaintext image and the ciphertext image.
2. Let \( d \) be the absolute difference between the two histograms obtained in Step 1.
3. Let \( d_i \) be the amplitude of histogram at index \( i \), then the sum of deviation can be calculated as follows [28]:

\[ D = \frac{d_0 + d_{255}}{2} + \sum_{i=1}^{254} d_i, \quad (7) \]

where \( d_0 \) and \( d_{255} \) are values of the difference histogram at index 0 and 255, respectively.
Higher the value of $D$, the encrypted image is more deviated from the original image [28]. By using Eq. 7 the sum of deviation between plaintext image and ciphertext image can be measured.

2) Irregular Deviation: Histogram deviation is a good parameter to judge the quality of an encryption algorithm, but we cannot depend on this factor alone. A good encryption algorithm should randomize the input pixels values in a uniform manner. This helps to prevent situations in which some pixels will undergo a large change while other pixels will undergo a small change from their initial values [30]. If the encryption algorithm treats the pixel values randomly, the statistical distribution of the deviation tends to be a uniform distribution. The irregular deviation measures how much the statistical distribution of histogram deviation is close to uniform distribution [30]. If Irregular deviation is close to uniform distribution then the encryption algorithm is said to be good [30]. The irregular deviation is:

1) Take the absolute difference of plaintext, $P$ image and the ciphertext, $C$ image [30].

$$D = |P - C|,$$  \hspace{1cm} (8)

2) Calculate the histogram of $D$.

$$H = \text{histogram}(D).$$ \hspace{1cm} (9)

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

$$M_H = \frac{1}{256} \sum_{i=0}^{255} h_i.$$ \hspace{1cm} (10)

4) Calculate the absolute of the histogram deviations from this mean value as follows: [30].

$$D_{H_i} = |h_i - M_H|.$$ \hspace{1cm} (11)

5) Now irregular deviation $I_D$ is calculated as follows [30].

$$I_D = \sum_{i=0}^{255} H_{D_i}.$$ \hspace{1cm} (12)

Smaller the value of $I_D$, better the encryption quality. Using Eq. 12 the lower value of $I_D$ indicates that the histogram distribution of the absolute deviation between the input and encrypted image is closer to the uniform distribution [30].

3) Deviation from Uniform Histogram: An ideal encryption algorithm encrypts an image in such a way that encrypted image must have a uniform histogram distribution [38]. In [38], a new encryption quality factor is proposed that describes a formula for deviation from an ideal assumed uniform histogram [38]. Let $H_C$ be the histogram of the ciphertext image and let $H_{C_i}$ be the value of the frequency of occurrence at index $i$, then uniform histogram is represented as [38]:

$$H_{C_i} = \begin{cases} \frac{M \times N}{256} & 0 \leq C_i \leq 255 \\ 0 & \text{elsewhere} \end{cases}$$ \hspace{1cm} (13)

The deviation from uniform histogram shown by Eq. 13 is calculated as [38]:

$$D_p = \frac{\sum_{C_i=0}^{255} |H_{C_i} - H_C|}{M \times N}.$$ \hspace{1cm} (14)

The lower value of $D_p$ represents better encryption quality because the lower value indicates that the histogram of ciphertext image is less deviated from uniform histogram and can be measured by Eq. 14.

4) Peak Signal-to-Noise Ratio (PSNR): Peak signal-to-noise ratio can be used to evaluate an encryption scheme. PSNR reflects the encryption quality. It is a measurement which indicates the changes in pixel values between the plaintext image and the ciphertext image [39]. Mathematically [39]:

$$\text{PSNR} = 10 \times \log_{10} \left( \frac{M \times N \times 255^2}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (P(i,j) - C(i,j))^2} \right),$$ \hspace{1cm} (15)

where $M$ is the width and $N$ is the height of digital image. $P(i,j)$ is pixel value of the plaintext image at grid $(i,j)$ and $C(i,j)$ is pixel value of the ciphertext image. The lower value of PSNR represents better encryption quality.

E. Diffusion Characteristics of a Cryptosystem

In cryptography, diffusion is a desirable property which is introduced by C.E Shannon in his paper, published in 1949 [33]. A good cryptosystem must ensure a good diffusion, means if one bit of the plaintext is changed, then the ciphertext should change completely, in an unpredictable manner. Diffusion characteristics of an image encryption algorithm means that the output pixels of ciphertext image should depend on the input pixels of plaintext image in a very complex way.

1) Avalanche Effect: A small change in key or plaintext image should cause significant change in the corresponding ciphertext image. This property of cryptosystem is known as avalanche effect. Avalanche effect is desirable property for all cryptographic algorithms. Strict avalanche effect occurs when a single bit change in the plaintext image change 50% of the bits in the ciphertext image. Mean Square Error (MSE) is the cumulative squared error between two digital images and can be used to check the avalanche effect. Let $C_1$ and $C_2$ be two ciphertext images whose corresponding keys are differ by one bit, then MSE can be calculated as [40], [41]:

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (C_1(i,j) - C_2(i,j))^2,$$ \hspace{1cm} (16)

where $M, N$ is the width and height of digital images and $C_1(i,j)$ is gray scale value of pixel at grid $(i,j)$ in cipher image $C_1$ and $C_2(i,j)$ is gray scale value of pixel at grid $(i,j)$ in cipher image $C_2$. In [42] the author discussed $MSE$ and generally speaking, if the value obtained using Eq. 16 for $MSE$ is $\geq 30$ dB, quality difference between two images is evident [42].

2) Number of Pixel Change Rate and Unified Average Change Intensity: For any encryption algorithm, it is desirable property that a small change in plaintext image should cause a significant change in the ciphertext image. Two common measures are used to check the influence of a one pixel change on the overall image. These two measures are Number of Pixel
Change Rate \((NPCR)\) and Unified Average Change Intensity \((UACI)\) \([14], [40], [43], [44]\).

Let \(C_1\) and \(C_2\) be two different cipher-images whose corresponding plaintext images are differ by only one bit. Label the gray scale 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. Define an array, \(D\), the same size as images \(C_1\) and \(C_2\). Then \(D(i,j)\) is determined by \(C_1(i,j)\) and \(C_2(i,j)\) namely if \(C_1(i,j) = C_2(i,j)\) then \(D(i,j) = 0\); otherwise, \(D(i,j) = 1\).

The \(NPCR\) is defined as \([14], [44]\):

\[
NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% ,
\]

where \(W\) and \(H\) are the width and height of ciphertext images \(C_1\) and \(C_2\).

By using Eq. 17, percentage of different pixel numbers between the plaintext image and the ciphertext image can be calculated. \(NPCR\) can also be defined as variance rate of pixels in the encrypted image caused by the change of a single pixel in the original image \([35]\).

Unified Average Change Intensity \((UACI)\) determines the average intensity of differences between the two images. Mathematically \(UACI\) can defined as \([40], [41]\):

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

The higher the value of \(NPCR\) and \(UACI\), the better the algorithm is.

### F. Effect of Noise

A good image cryptosystem should work in noisy environment and should be robust against noise. But in the literature some encryption scheme exists that are very sensitive against noise \([3], [4]\). The noise resistance capability shows the ability of an image cryptosystem to tolerate noise. Noise with different SNR is added in encrypted image to check noise immunity. If decrypted image is very close to the original image, visually or numerically (correlation coefficient near to one), then the cryptosystem is immune against noise.

### G. Key Space Analysis

A good image encryption algorithm should be sensitive to cipher keys \([45]\). Key space analysis is summarized in the following Section \([45]\).

1) **Exhaustive Key Search:** An encryption scheme is considered secure if its key space is large enough. With a large key space, some attacks on encryption scheme are made infeasible \([27], [45]\). Attacks like brute force attack are made infeasible when key space is large. Let us suppose that an encryption algorithm has \(k\)-bit key. An exhaustive key search will require \(2^k\) operations to succeed. This is very large because an attacker needs to try all possible keys. Let us suppose the key size is 128 bit, then an attacker needs \(2^{128}\) operations to find the exact key. If the attacker employs a 1000 MIPS computer to guess the key by brute force attack, the computational load in year is;

\[
\frac{2^{128}}{1000 \times 10^6 \times 60 \times 60 \times 24 \times 365} > 10.7902831 \times 10^{21} \text{ years}. \tag{19}
\]

This is very long time and practically infeasible \([27]\).

2) **Key Sensitivity Test:** Another test with respect to secret key is the key sensitivity test that indicates how much an encrypted image is sensitive towards the change in the key. For a secure cryptosystem, a decryption algorithm will not decrypt ciphertext image correctly, even if there is a one bit difference between key \([46]\). It means that large key sensitivity is required for highly secure cryptosystems. An ideal image encryption should be sensitive with respect to the secret key such that a single bit change in the key should produce a completely different encrypted image \([46]\).

### H. Cryptanalysis

An encryption scheme is designed to keep plaintext secret from an attacker, while cryptanalysis is the science of recovering plaintext without access to the key. Cryptology encompasses the area of cryptography and cryptanalysis. It is also called code-cracking or code-breaking. An assumption is necessary during cryptanalysis process that details of cryptosystems and complete knowledge of an encryption scheme is known to cryptanalyst \([47], [48]\). To find a weakness in ciphertext, code or key management scheme, is known as attack. In short an attempted cryptanalysis is called an attack. The following attacks are used to break a cryptosystem \([47], [48]\).

1) **Ciphertext only Attack:** In this type of attack, the cryptanalyst has access to a set of ciphertext. In ciphertext only attack, encryption algorithm and ciphertext is known to an attacker. An attacker tries to break the algorithm or in simple words tries to deduce the decryption key or plaintext by observing the ciphertext \([3], [47], [48]\). A cryptosystem completely fails if the corresponding plaintext or key is deduced by an intruder. The main objective of the attack is to recover the plaintext and or the secret key.

2) **Known Plaintext Attack:** The attacker has access to one or more ciphertext and the corresponding plaintext messages. The objective is to find the secret key \([3]\).

3) **Chosen Plaintext Attack:** In this attack, the attacker has liberty to choose a plaintext of his/her choice and get the corresponding ciphertext. Since the attacker can choose plaintext of his/her choice, this attack is more powerful. Again the objective of this attack is to find the secret key. If the underlying encryption mechanism is weak, chosen plaintext attack can disclose the key, which is being used in the encryption process.

4) **Chosen Ciphertext Only Attack:** The attacker can choose ciphertext and get the corresponding plaintext. By selecting some ciphertext a cryptanalyst has access to corresponding decrypted plaintext. Chosen ciphertext only attack is more applicable to public key cryptosystems \([3]\).
TABLE I: Average time required for exhaustive key search [28].

<table>
<thead>
<tr>
<th>Key Size (bits)</th>
<th>Number of Alternative Keys</th>
<th>Time required at $10^6$ Decryption/µs</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>$2^{32} = 4.3 \times 10^9$</td>
<td>2.15 milliseconds</td>
</tr>
<tr>
<td>56</td>
<td>$2^{56} = 7.2 \times 10^{16}$</td>
<td>10 hours</td>
</tr>
<tr>
<td>128</td>
<td>$2^{128} = 3.4 \times 10^{38}$</td>
<td>5.4 $\times 10^{18}$ years</td>
</tr>
<tr>
<td>256</td>
<td>$2^{256} = 3.7 \times 10^{50}$</td>
<td>5.9 $\times 10^{30}$ years</td>
</tr>
</tbody>
</table>

5) **Brute Force Attack:** In this type of attack, a cryptanalyst tries all possible keys in finite key space one by one and check the corresponding plaintext, if meaningful. The basic objective of a brute force attack is to try all possible combinations of the secret key to recover the plaintext image and or the secret key. On an average, half of all possible keys must be tried to achieve success but brute force attack involves large computation and has a very high complexity. Due to high complexity brute force attack may not be feasible. Table I shows how much time is involved for various key space [49].

### III. EVALUATION OF AES AND CFES

The parameters investigated in Section II are used for the evaluation of AES and CFES. In this Section, correlation coefficient analysis, information entropy analysis, compression friendliness, encryption quality measurement, diffusion characteristics, key space analysis, effect of JPEG compression and effect of noise on both AES and CFES is explored.

#### A. Overview of CFES

In [26], the authors presented a Compression Friendly Encryption Scheme (CFES), which is based on a number of interesting properties of orthogonal matrix. Block diagram of the CFES is shown in Fig. 1 [26]. The encryption process of CFES can be summarized as follows. First of all, DCT of plain-text ($P_i$) is taken to get frequency domain image ($Y_i$). Then frequency domain image ($\Lambda Y_i$) is multiplied with orthogonal matrix ($\Phi_i$) to get $X_i$. Permutation function is applied on $X_i$ and a permuted image ($\tilde{Y}_i$) is obtained. Inverse DCT of permuted image ($\tilde{Y}_i$) is taken to get spatial domain image ($\tilde{P}_i$). The last step of encryption process in CFES is scaling of $\tilde{P}_i$ and cipher-text image ($C_i$) is obtained. To decrypt the cipher-text image ($C_i$), the transformation used in the encryption algorithm are applied in the reverse order, as shown in Fig. 1.

#### B. Correlation Coefficient Analysis

Correlation is a measure that computes degree of similarity between two variables. In this section, we present correlation coefficient analysis on AES and CFES. The correlation coefficient (degree of similarity) between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in original and cipher image were tested. The testing was done by randomly selecting 1000 pairs of two adjacent pixels (in vertical, horizontal and diagonal direction) from the original and corresponding cipher image. Correlation coefficient was calculated using Eq. 1. Tests were performed on Cameraman, Baboon, Nike and Goldhill images. The size of all the four images were $256 \times 256$ pixels. Figure 2 shows the correlation distribution of two horizontally adjacent pixels in the plaintext images and ciphertext images, where plaintext image was the Cameraman image. In case of AES, the horizontal correlation coefficients are 0.9282 for plaintext image and -0.0067 for AES encrypted image, which are far apart. In case of plaintext image the value of horizontal correlation coefficient is 0.9282 which is near to 1 (maximum correlation) whereas for AES encrypted image the horizontal correlation is -0.0067, which means that encrypted image is uncorrelated in horizontal direction. Similar results for diagonal and vertical directions were obtained as shown in Table II. For Cameraman image, it is clear from the Fig. 2 and Table II that there is negligible correlation between the two adjacent pixels in the cipher-image, in case of AES. However, the two adjacent pixels in the plaintext image are highly correlated. When Cameraman image was encrypted using CFES, correlation coefficients are 0.0124 and 0.0202 in vertical and diagonal direction, respectively. However, the correlation coefficient in horizontal direction is 0.9522, which means that image encrypted by CFES has high correlation in horizontal direction. Correlation in horizontal direction plays an important role in JPEG compression which will be discussed later in this paper. Similar results are obtained for Baboon, Nike and Goldhill images which are shown in Table III, Table IV, Table V, respectively. It is clear from Table II to Table V that for plaintext images, the value of correlation coefficient in all directions is close to 1. The ciphertext images obtained using the AES algorithm has correlation coefficient close to zero all directions. However, in case of the CFES the correlation coefficient in vertical and diagonal directions is close to zero but the correlation coefficient in the horizontal direction is close to 1. This is due to multiplication of the input image by orthogonal matrices. Despite the fact that the CFES scheme yields high correlation in the horizontal direction,
TABLE II: Correlation coefficient of two adjacent pixels: Cameraman image.

<table>
<thead>
<tr>
<th>Direction of adjacent pixels</th>
<th>Plain Image AES</th>
<th>Plain Image CFES</th>
<th>Cipher Image AES</th>
<th>Cipher Image CFES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizontal</td>
<td>.9282</td>
<td>0.9282</td>
<td>-0.0067</td>
<td>0.9522</td>
</tr>
<tr>
<td>Vertical</td>
<td>.9644</td>
<td>0.9644</td>
<td>0.0504</td>
<td>0.0124</td>
</tr>
<tr>
<td>Diagonal</td>
<td>.9116</td>
<td>0.9116</td>
<td>-0.0156</td>
<td>0.0202</td>
</tr>
</tbody>
</table>

TABLE III: Correlation coefficient of two adjacent pixels: Baboon image.

<table>
<thead>
<tr>
<th>Direction of adjacent pixels</th>
<th>Plain Image AES</th>
<th>Plain Image CFES</th>
<th>Cipher Image AES</th>
<th>Cipher Image CFES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizontal</td>
<td>.7103</td>
<td>0.7103</td>
<td>-0.037</td>
<td>0.9547</td>
</tr>
<tr>
<td>Vertical</td>
<td>.5966</td>
<td>.5966</td>
<td>0.0107</td>
<td>0.0611</td>
</tr>
<tr>
<td>Diagonal</td>
<td>.6225</td>
<td>0.6225</td>
<td>-0.0419</td>
<td>-0.0025</td>
</tr>
</tbody>
</table>

TABLE IV: Correlation coefficient of two adjacent pixels: Nike image.

<table>
<thead>
<tr>
<th>Direction of adjacent pixels</th>
<th>Plain Image AES</th>
<th>Plain Image CFES</th>
<th>Cipher Image AES</th>
<th>Cipher Image CFES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizontal</td>
<td>.9605</td>
<td>0.9605</td>
<td>-0.0253</td>
<td>0.9144</td>
</tr>
<tr>
<td>Vertical</td>
<td>.9009</td>
<td>.9009</td>
<td>-0.0197</td>
<td>0.0216</td>
</tr>
<tr>
<td>Diagonal</td>
<td>.9101</td>
<td>0.9101</td>
<td>-0.0030</td>
<td>-0.0011</td>
</tr>
</tbody>
</table>

TABLE V: Correlation coefficient of two adjacent pixels: Goldhill image.

<table>
<thead>
<tr>
<th>Direction of adjacent pixels</th>
<th>Plain Image AES</th>
<th>Plain Image CFES</th>
<th>Cipher Image AES</th>
<th>Cipher Image CFES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizontal</td>
<td>.9519</td>
<td>0.9519</td>
<td>-0.0407</td>
<td>0.9604</td>
</tr>
<tr>
<td>Vertical</td>
<td>0.9391</td>
<td>0.9391</td>
<td>-0.0067</td>
<td>0.0152</td>
</tr>
<tr>
<td>Diagonal</td>
<td>0.8993</td>
<td>0.8933</td>
<td>0.0463</td>
<td>-0.0113</td>
</tr>
</tbody>
</table>

however it does not leak any information that could be used to guess the plaintext image or the secret key.

C. Information Entropy Analysis

As discussed in Section II, ideally the information entropy should be 8 bits for gray scale images. If an encryption scheme generates an output cipher image whose entropy is less than 8 bits, then there would be a possibility of predictability, which may threaten its security [34], [35]. Information entropy is calculated by using Eq. 6. Simulation results for entropy analysis are shown in Table VI. For AES, the value of entropy is very close to theoretical value of 8 bits. This implies that information leakage is negligible and AES encryption algorithm is secure against entropy attack. But CFES has less entropy i.e. approximately 7 bits as compare to AES.

D. Compression Friendliness

As discussed in the previous section, an algorithm is said to be compression friendly if size of the encrypted image is same as that of the plaintext image [18], [37]. So both AES and

![Fig. 2: Correlation in original Cameraman image.](image1)

![Fig. 2: Correlation in AES encrypted Cameraman image.](image2)

![Fig. 2: Correlation in CFES encrypted Cameraman image.](image3)
CFES are compression friendly because both algorithms do not increase the size of encrypted image. To check this property Cameraman, Baboon, Nike and Goldhill images of 65 kB were encrypted using the AES and CFES. The size of cipher image was 65 kB. Both AES and CFES are compression friendly because the size of cipher images was same as plaintext images.

### E. Encryption Quality Measurement

The effectiveness of an encryption algorithm can be judged by visual inspection but this not sufficient. In some cases, visual inspection is cannot determine the amount of information concealed by the encryption algorithm [24], [30]. So deviation in pixels values between plaintext image and ciphertext image is a good parameter to judge the encryption quality. To check deviation in pixels, maximum deviation and irregular deviation is used as quality measurement for both the AES and CFES. If histogram of an encrypted image is uniform, i.e., each gray level has equal probability, then encryption scheme is more robust against different attacks and the quality of scheme is high [38]. Maximum deviation, irregular deviation and histogram uniformity are calculated using Eq. 7, 12 and 14 respectively. In [38], the author proposed a new parameter to judge the quality of encryption scheme, which is discussed in Section II. Simulation results are shown in Table VII for both AES and CFES.

As discussed in Section II, the value of maximum deviation ($D$) should be high so that encrypted image will be more deviated from the corresponding original image. For all the test images, the value of maximum deviation ($D$) in AES encrypted images is higher than CFES which is shown in Table VII. From Table VII it is clear that image encrypted by CFES is less deviated from the original image. If the value of irregular deviation ($I_D$) is smaller, then encryption quality is better which means that lower value of irregular deviation ($I_D$) is required [30]. Comparing the value of irregular deviation ($I_D$) for both AES and CFES using Table VII, the value of irregular deviation ($I_D$) for AES is lower than CFES. So, irregular deviation ($I_D$) test shown in Table VII indicates that AES encrypted image is better than image encrypted by CFES. The metric proposed in [38] measures the quality of encryption in terms of how the encryption algorithm minimizes the deviations of the encrypted image from an assumed ideal encryption case. For an ideally encrypted image (ciphertext), $C$ must have a completely uniform histogram distribution. In fact, encryption quality is better if the value of $D_p$ is lower [38]. From Table VII, it is clear that AES encrypted images have less $D_p$ than CFES which indicates that AES encrypted images are less deviated from assumed ideal histogram.

### F. Diffusion Characteristics of Cryptosystems

1) Avalanche Effect: Avalanche effect is a desirable property for a cryptographic algorithm. For testing of diffusion characteristics, avalanche effect metric is used [40]. Avalanche effect is evident if a slight change in input causes significant changes in the output. In good cryptosystems, a small change in the key or plaintext should causes a significant change in ciphertext. To test the efficiency of diffusion mechanism, a single bit change can be made in the plaintext image $P$ to give a modified image, $\bar{P}$. Both $P$ and $\bar{P}$ are encrypted to give $C$ and $\bar{C}$, respectively. A good diffusion algorithm is guaranteed if $C$ and $\bar{C}$ differ from each other in half of their bits [40], [41]. If the changes are small, this might provide a way to reduce the size of the key space to be searched [40], [41].

Figure 3 shows the diffusion test result of difference test for Cameraman image using the AES. When original Cameraman image and one bit change Cameraman was encrypted using the AES, both encrypted images seems similar which are shown in Fig. 3 (b) and Fig. 3 (c), respectively. However, when the difference of Fig. 3 (b) and Fig. 3 (c) is taken, quality difference is found as shown in Fig. 3 (d). Now original and one bit change Cameraman images are encrypted using CFES, which is shown in Fig. 4. From visual perception, by using Fig. 4 (b) and Fig. 4 (c), it is not clear that both figures are similar or different, so the difference of both encrypted images have been taken. Result is shown in Fig. 4 (d). From Fig. 4 (d) it is clear that CFES has less diffusion characteristics as compared to the AES. Similar results were obtained for Baboon, Nike, and Goldhill image which is shown in Fig. 5, Fig. 6 and Fig. 7 respectively.

Mean Square Error (MSE) can be used to check the avalanche effect. MSE can be calculated by Eq. 16, which is discussed in Section II. If $MSE \geq 30 \text{ dB}$, quality difference between two images is evident [42]. To check the influence of one pixel change, tests were performed on Cameraman, Baboon, Nike, and Goldhill images. Simulation results are shown in Table VIII for both AES and CFES, the MSE is $> 30 \text{ dB}$, the ciphertexts are significantly different when plaintext differs by one pixel. For AES, quality differences are more than CFES, which is shown in Table VIII.

2) NPCR and UACI: Two common measures are used to check the influence of one pixel change on the whole image, encrypted by an algorithm. The two tests are Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity.
TABLE VIII: MSE results.

<table>
<thead>
<tr>
<th>Encrypted Image</th>
<th>AES</th>
<th>CFES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cameraman</td>
<td>40.39 dB</td>
<td>33.86 dB</td>
</tr>
<tr>
<td>Baboon</td>
<td>40.34 dB</td>
<td>33.31 dB</td>
</tr>
<tr>
<td>Nike</td>
<td>40.41 dB</td>
<td>33.04 dB</td>
</tr>
<tr>
<td>Goldhill</td>
<td>40.37 dB</td>
<td>33.50 dB</td>
</tr>
</tbody>
</table>

TABLE IX: Avalanche effect results.

<table>
<thead>
<tr>
<th>Images</th>
<th>AES NPCR</th>
<th>AES UACI</th>
<th>CFES NPCR</th>
<th>CFES UACI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cameraman</td>
<td>99.60</td>
<td>33.53</td>
<td>99.12</td>
<td>15.49</td>
</tr>
<tr>
<td>Baboon</td>
<td>99.62</td>
<td>33.36</td>
<td>99.09</td>
<td>15.39</td>
</tr>
<tr>
<td>Nike</td>
<td>99.64</td>
<td>33.60</td>
<td>99.09</td>
<td>14.01</td>
</tr>
<tr>
<td>Goldhill</td>
<td>99.62</td>
<td>33.58</td>
<td>99.18</td>
<td>14.84</td>
</tr>
</tbody>
</table>

(UACI). NPCR measures the percentage of the number of different pixel to the total number of pixels. In short NPCR means the number of pixels change rate of ciphered image while one pixel of plaintext image is changed. To check the average intensity of differences between the images, UACI is used. To check the influence of one pixel change, tests were performed on Cameraman, Baboon, Nike and Goldhill images. Simulation results are shown in Table IX. The higher the value of NPCR and UACI, the better the encryption algorithm is. From Table IX, it is clear that AES has good diffusion characteristics than CFES. With respect to the NPCR and UACI, results in Table IX, the CFES has less sensitivity to small changes in plaintext images, but the AES is highly sensitive to small changes in plaintext image. Generally, these obtained results show that the AES has strong diffusion mechanism as compare with the CFES.

G. Key Space Analysis

A good image encryption algorithm should be sensitive to the cipher keys [27]. The key space analysis and test for AES and CFES are summarized in the following Sections.
(a) Difference of original encrypted Nike image and 1 bit changed encrypted Nike image for AES.

(b) Difference of original encrypted Nike image and 1 bit changed encrypted Nike image for CFES.

Fig. 6: Results of the difference test for both AES and CFES: Nike image.

(a) Difference of original encrypted Goldhill image and 1 bit changed encrypted Goldhill image for AES.

(b) Difference of original encrypted Goldhill image and 1 bit changed encrypted Goldhill image for CFES.

Fig. 7: Results of the difference test for both AES and CFES: Goldhill image.

1) Exhaustive Key Search: For AES the key space is $10^k$, where $k$ is key size in bits. AES uses a key of 128, 192 or 256 bits, so key space is large enough to resist all types of brute force attack. An exhaustive key search will take $2^k$ operation to succeed. Like AES, CFES also uses 128 bit key length. So an attacker need about $2^{128}$ operations to successfully determine the key. If an opponent employs a 1000 MIPS computer to guess the key by the brute force attack, the computational load in years is:

$$\frac{2^{128}}{1000 \times 10^9 \times 60 \times 60 \times 24 \times 365} > 10.7902831 \times 10^{21} \text{ years}$$

(20)

2) Key Sensitivity Test: Let $C_1$ and $C_2$ be two different cipher images whose corresponding keys differ by only one bit. Then the percentage difference between two ciphertexts is calculated, whose corresponding keys are differ by one bit. Simulations results are shown in Table X. From Table X it is concluded that the AES and CFES are very sensitive with respect to key sensitivity test, more than 99% changes occurs when cipher keys are different.

H. Effect of JPEG Compression on AES and CFES

Lossy compression is usually employed for multimedia data to save bandwidth and storage space. An interesting property of CFES is that, it is JPEG compression tolerant encryption scheme [26]. It means that CFES is able to reconstruct the plaintext image even if the encrypted image is JPEG compressed. CFES can also generate encrypted images with varying perceptual distortion. In case of AES, when encrypted image data undergoes JPEG lossy compression, the decryption algorithm cannot recover the plaintext image. Because conventional algorithm like AES are designed to recover the exact value of plaintext data stream, they cannot work under lossy compression environment.

For multimedia data application, an approximation of original image is sufficient as long as the error between the original image and recovered image is small. CFES recovers an approximation of the plaintext image from the encrypted image with a good perceptually similarity with respect to original plaintext image. When an image is encrypted using AES algorithm and then encrypted image undergoes JPEG lossy compression, the size of encrypted image increases. AES encrypted image is highly uncorrelated, which means that ciphertext of AES have negligible correlation between pixels values. When an uncorrelated image is JPEG compressed, size of image increases instead of reducing.

Response of AES and CFES to JPEG compression for all four images are shown from Fig. 9 to Fig. 12. To show the response of AES and CFES for different quality factors, simulation was carried out and the results are shown in Table XI and XII. The size of original image was 65 kB. In case of CFES, when an image is encrypted and undergoes JPEG lossy compression, size of the image is always less than size of original image. CFES encrypted image has correlation in horizontal direction, due to this correlation, the encrypted image can be compressed using JPEG compression. But for AES when encrypted image was JPEG compressed for QF =100, the size of the encrypted image was 101 kB as shown in Table 8. The size of AES encrypted image increases due to the fact that AES encrypted image has very less correlation; approximately zero.

From Fig. 9 to Fig.12, it is proved that when AES encrypted image undergoes JPEG lossy compression, original image cannot be recovered after JPEG lossy compression. But in case of CFES, the original image can be recovered even if the encrypted image is JPEG compressed. Figure 8 shows the size of image for different quality factors both for AES and CFES. Figure 8 shows that CFES has better results as compared to AES. The results shown in Table XI indicates that when quality factor of JPEG lossy compression decreases, then size of encrypted image also decreases.

<table>
<thead>
<tr>
<th>Encrypted Image</th>
<th>AES</th>
<th>CFES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cameraman</td>
<td>99.5880%</td>
<td>99.2554%</td>
</tr>
<tr>
<td>Baboon</td>
<td>99.6506%</td>
<td>99.1882%</td>
</tr>
<tr>
<td>Nike</td>
<td>99.5956%</td>
<td>99.1013%</td>
</tr>
<tr>
<td>Goldhill</td>
<td>99.5987%</td>
<td>99.2279%</td>
</tr>
</tbody>
</table>

TABLE X: Difference of two ciphers when keys differ by one bit.
Fig. 8: Comparison of AES and CFES when an image of size 65kB is JPEG compressed.

(a) Decrypted output when AES encrypted image was JPEG compressed with QF =100.

(b) Decrypted output when CFES encrypted image was JPEG compressed with QF =100.

Fig. 9: Response of AES and CFES to JPEG compression using Cameraman image as test image.

(a) Decrypted output when AES encrypted image was JPEG compressed with QF =100.

(b) Decrypted output when CFES encrypted image was JPEG compressed with QF =100.

Fig. 10: Response of AES and CFES to JPEG compression using Baboon image as test image.

(a) Decrypted output when AES encrypted image was JPEG compressed with QF =100.

(b) Decrypted output when CFES encrypted image was JPEG compressed with QF =100.

Fig. 11: Response of AES and CFES to JPEG compression using Nike image as test image.

I. Effect of Noise on AES and CFES

A good encryption scheme should be resistant against noise. The effect of noise on AES and CFES is studied in this section. AWGN with different SNR is added in encrypted images. After addition of AWGN, the decryption is performed on noisy images. The test results shown from Fig. 13 to Fig. 14, reveals that the AES algorithm is very sensitive to noise. So, AES is not suitable for noisy environment. From simulation results it is clear that CFES is more robust to noise and can work in noisy environment. In case of CFES, PSNR of decrypted images also varies with variation of SNR, which is shown in

TABLE XI: Size of encrypted image after CFES algorithm when image undergoes JPEG lossy compression.

<table>
<thead>
<tr>
<th>JPEG QF</th>
<th>Cameraman image</th>
<th>Baboon image</th>
<th>Nike image</th>
<th>Goldhill image</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>49.3kB</td>
<td>50.5kB</td>
<td>55.4kB</td>
<td>45.2kB</td>
</tr>
<tr>
<td>90</td>
<td>21.1kB</td>
<td>22.1kB</td>
<td>24.4kB</td>
<td>18.6kB</td>
</tr>
<tr>
<td>80</td>
<td>15.1kB</td>
<td>15.0kB</td>
<td>16.9kB</td>
<td>13.9kB</td>
</tr>
<tr>
<td>70</td>
<td>13.0kB</td>
<td>12.9kB</td>
<td>14.1kB</td>
<td>12.3kB</td>
</tr>
<tr>
<td>60</td>
<td>11.5kB</td>
<td>11.5kB</td>
<td>12.4kB</td>
<td>11.0kB</td>
</tr>
<tr>
<td>50</td>
<td>10.7kB</td>
<td>10.6kB</td>
<td>11.2kB</td>
<td>10.2kB</td>
</tr>
<tr>
<td>40</td>
<td>9.2kB</td>
<td>9.8kB</td>
<td>10.1kB</td>
<td>10.2kB</td>
</tr>
<tr>
<td>30</td>
<td>8.8kB</td>
<td>8.8kB</td>
<td>8.9kB</td>
<td>8.5kB</td>
</tr>
<tr>
<td>20</td>
<td>7.3 kB</td>
<td>7.2kB</td>
<td>7.2kB</td>
<td>6.9kB</td>
</tr>
<tr>
<td>10</td>
<td>4.9kB</td>
<td>4.9kB</td>
<td>4.8kB</td>
<td>4.7kB</td>
</tr>
</tbody>
</table>

TABLE XII: Size of AES encrypted image after JPEG compression.

<table>
<thead>
<tr>
<th>JPEG QF</th>
<th>JPEG Compressed File</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>101.0kB</td>
</tr>
<tr>
<td>90</td>
<td>50.5kB</td>
</tr>
<tr>
<td>80</td>
<td>39.1kB</td>
</tr>
<tr>
<td>70</td>
<td>33.7kB</td>
</tr>
<tr>
<td>60</td>
<td>30.1kB</td>
</tr>
<tr>
<td>50</td>
<td>27.6kB</td>
</tr>
<tr>
<td>40</td>
<td>24.9kB</td>
</tr>
<tr>
<td>30</td>
<td>21.7kB</td>
</tr>
<tr>
<td>20</td>
<td>17.0kB</td>
</tr>
<tr>
<td>10</td>
<td>12.2kB</td>
</tr>
</tbody>
</table>

Table: Size of encrypted image after CFES algorithm when image undergoes JPEG lossy compression.

Table: Size of AES encrypted image after JPEG compression.

I. Effect of Noise on AES and CFES

A good encryption scheme should be resistant against noise. The effect of noise on AES and CFES is studied in this section. AWGN with different SNR is added in encrypted images. After addition of AWGN, the decryption is performed on noisy images. The test results shown from Fig. 13 to Fig. 14, reveals that the AES algorithm is very sensitive to noise. So, AES is not suitable for noisy environment. From simulation results it is clear that CFES is more robust to noise and can work in noisy environment. In case of CFES, PSNR of decrypted images also varies with variation of SNR, which is shown in...
(a) Decrypted output when AES encrypted image was JPEG compressed with QF =100.

(b) Decrypted output when CFES encrypted image was JPEG compressed with QF =100.

Fig. 12: Response of AES and CFES to JPEG compression using Goldhill image as test image.

(a) Decryption result for AES encrypted Cameraman image.

(b) Decryption result for CFES encrypted Cameraman image.

(c) Decryption result for AES encrypted Baboon image.

(d) Decryption result for CFES encrypted Baboon image.

(a) Decryption result for AES encrypted Nike image.

(b) Decryption result for CFES encrypted Nike image.

(c) Decryption result for AES encrypted Goldhill image.

(d) Decryption result for CFES encrypted Goldhill image.

Fig. 14: Effect of noise on AES and CFES when SNR = 50 dB.

Fig. 15: Variation of the PSNR of decrypted image with SNR of encrypted image for AES and CFES.

In this paper, a number of evaluation parameters proposed in the literature were systemically presented to form a frame work for evaluating image encryption algorithms. AES and CFES were compared with each other. The base of comparison for both the algorithms were those parameters which were investigated in Section II. Comparison is carried out with respect to different parameters like, correlation coefficient, information entropy, compression friendliness, NPCR and UACI. In correlation coefficient analysis, the image encrypted by CFES has correlation in horizontal direction while AES encrypted image has very less correlation in all directions. Less correlation values indicates higher security. The horizontal correlation in CFES plays an important role because it helps to JPEG compress encrypted images. On the other hand an AES encrypted image has less correlation in all directions, however the size of an AES encrypted image increases if it is subjected to JPEG compression.

Entropy values for CFES were less as compared to AES, however looking at the structure of CFES encrypted image it appears that it does not leak any information about that plaintext. No overheads or very less overheads are needed for
both algorithms so both schemes are compression friendly. The encryption quality of CFES was less when comparison was carried out with AES. During avalanche effect test, AES proved good diffusion characteristics while CFES has less diffusion. The value of NPCR and UACI was very high for AES.

Noise immunity is distinguishable property of CFES. When image is encrypted using CFES, the decryption algorithm can recover the plaintext image even the ciphertext is corrupted by noise. But when AES encrypted image was corrupted by noise the decryption algorithm was unable to recover the original plaintext image.

REFERENCES


Jawad Ahmad received the B.E degree from Muhammad Ali Jinnah University, Islamabad, Pakistan, in 2009. He is currently pursuing the MS degree at the HITEC University, Taxila Cantt, Pakistan. From 2010 to date, he is working as a junior lecturer at HITEC university, Taxila Cantt, Pakistan. His research interests include image processing, cryptography and mobile communication.

Fawad Ahmed received BE degree in Industrial Electronics from Institute of Industrial Electronics Engineering, NED University of Engineering and Technology, Karachi in 1995, MS degree in Systems and Controls from The University of New South Wales Australia in 1998 and PhD degree from Nanyang Technological University, Singapore in 2010. Dr. Ahmed’s research interests include digital watermarking, image authentication using robust hashing, image encryption, biometrics, and cryptography. He has around 16 years of experience that spans industry, research and teaching. He has received various scholarships and the best teacher award in the year 1999/2000. Dr. Ahmed has taught various courses in the area of Electronics, Instrumentation, Digital image processing, MATLAB programming and Microcontroller programming & Interfacing. The bibliography of Dr. Ahmed has been included in the 2009 Edition of Who’s Who in the World.