Chapter 3

Performance Assessment Metrics

3.1. Overview

This chapter discusses different performance assessment metrics which are considered for assessing the performances of user authentication and encryption approaches developed by different researchers in authentication, text and image domain. Some of the well known standard techniques, tools and parameters are deliberated for assessing the performance of newly implemented schemes relating to user authentication, text encryption and image encryption domain.

Section 3.2 briefly describes different performance assessment metrics which are applied to assess the performances of newly developed schemes from authentication, text and image domain. Conclusion regarding assessment metrics for the respective domain is drawn in section 3.3.

3.2. Performance Assessment Matrices

This section describes different performance assessment metrics which are applied to measure the superiority of the newly implemented user authentication, text encryption and image encryption schemes. Different well known standard encryption schemes, attacks, tools and parameters are described in this aspect.

3.2.1. Different Cryptographic Attacks

Different types of cryptographic attacks [18][73][76][86][93] which are considered for accessing the security of newly implemented user authentication algorithms have been described here.

A. Brute force Attack

Brute force attack is based on trial and error method in which attempts are made to gain access to secret information by exhaustively applying all possibilities repeatedly. This is a simple method where the focus is given in repeated guessing rather than using intellectual strategies. Normally automated software is used to make repeated attempts by consecutive guessing. The attacker tries to get some form of password and attacks with all possible combinations to access the secret data.

B. Dictionary Attack

Dictionary attack is a technique, which attempts to gain access over an authentication mechanism by inputting each word from a dictionary as a password. By using a similar process, a dictionary attack is able to determine the decryption key, which is used to generate an encrypted message. Applying of strong password policy at the time of password creation may protect the system over dictionary attack.

C. Key Logger Attack

Key logger is a software program or hardware which surveillance and records all the keystrokes made from a specific keyboard without the knowledge of the user. In that manner, the key logging program captures the entire keystrokes related to secret information. A strong password is not able to protect this attack as all the keystrokes are compromised thus need multi-factor authentication for protection.

D. Man in the Middle Attack

This kind of attack is carried out to intercept secret information transmitting through two communicating people. In this kind of attack, an attacker is logically present and hiding its existence from client and server. Sender and receiver share secret information as they believe that they are communicating directly but the intruder intercepts all secret credentials and security of the system is compromised. This attack is commonly used to steal financial and personal information. Using certificates, encrypted data transmission protocols can be considered as protection over this attack.

E. Physical Access to Phone

In this kind of attack, all the secret information like SMS message, OTP (One Time Password) is compromised as attacker have the physical access to a phone. This kind of attack is carried out in not on a large scale as gaining physical access of phone is hard to achieve. Application tools are available in the market to extract data from mobile phones.

F. Mobile Phone Trojans

The malware and Trojans are developed specifically for mobile phones which can intercept all incoming and outgoing SMS messages containing user personal information and OTPs in an unauthenticated manner. Normally these kinds of attacks [63] are carried out for financial frauds. Strong antivirus might be able to protect this kind of attack.

G. Phishing Attack

Phishing attack is carried out to steal financial document information, login credentials and other secret information. An attacker convinces a victim to open a text message, email or instant message. As the victim clicks into a malicious link, malware is installed automatically which either freeze the system or extract the secret information.

3.2.2. CrypTool

CrypTool is free e-learning software from cryptographic field which includes most of the cryptographic functions as well as cryptanalytic concepts. Around 400 cryptographic algorithms are implemented with the facility of graphical user interface, online help, analytical tools and adjustment of user own parameters by CrypTool [19].

The development for implementing the CrypTool is started in 1998 where it becomes open source software from 2001. The main purpose of this project is to explain the different cryptographic concepts and the security provided by the algorithms over network threats. CrypTool is applied mainly in the field of computer science, mathematics and business computing.

Most of the Classical, symmetric and asymmetric cryptographic algorithms are implemented in CrypTool. Different algorithms like RSA, AES, DES, Triple DES, ECC, Serpent, Blowfish, Twofish and other cryptographic algorithms are implemented by this tool. Hybrid and homomorphic encryptions, digital signatures are also explained in this tool. Additional functions like Hash generation, ECC demonstration etc and tutorials module on different topics like number theory and others are also included in CrypTool. CrypTool is awarded by several international awards for its contribution in the field of cryptography.

3.2.3. Triple DES

Triple Data Encryption Algorithm or Triple DEA or 3DES is a block cipher with the presence of symmetric secret key which is constructed based on the concept of DES. Triple DES is introduced in 1998 and it is considered as a standard ANS X9.52. Each data block is encrypted by DES algorithms for three times in Triple DES [82].

In Triple DES length of the block is 64 bits where the length of the key is 56 or 112 or 168 bits. Key with 112 bits provides effective security for Triple DES. Triple DES uses the Feistel network structure and 48 DES equivalent rounds.

Three numbers of keys with a length of 64-bits each are taken as input. A user may input the entire 24 characters (192-bits) key all together rather than inputting three keys separately. In Triple DES, the user inputted keys are divided into three sub keys. Padding is applied for each of the subkeys if necessary. Thus three subkeys with a length of 64-bit each are generated. Encryption algorithm of regular DES is applied here but the procedure is repeated for three times. Data encryption is carried out with the help of the first key where the second key is considered for decryption. Final encryption is done by the third key.

Triple DES provides more security compare to regular DES but the speed of encryption for Triple Des is much slower rather than regular DES.

3.2.4. Advanced Encryption Standard

Advanced Encryption Standard (AES) is a symmetric block cipher which is also known by its original name Rijndael as it is a subset of Rijndael ciphers. AES is extremely faster than DES and with a larger key size. AES is considered as encryption specification standard for electronic data.

AES is based on the principle of substitution-permutation network and AES needs less execution time for software as well as for hardware. AES is an iterative cipher with a fixed block size of 128 bits. The key size of AES is 128, 192 or 256- bits.

AES applies variable numbers of rounds depending upon the key length where 10, 12 and 14 rounds are used for 128-bit, 192-bit and 256-bit keys respectively. Each round of encryption of AES is carried out by performing four subprocesses which are Byte

substitution, Shift rows, Mix columns and Add round key. Decryption is carried out by performing all these subprocesses in reverse sequence.

Implementation and strength of AES keys for key length 128-bits, 192-bits and 256-bits are very high that it is able to protect the secret information from unauthorized accesses. High key lengths of 192-bits, 256-bits are applied to protect very secret information. Proper implementation and key management assure the security provided by AES [29][57].

3.2.5. Serpent Algorithm

The serpent is a block cipher where the symmetric key is applied. Serpent ensures high security but it lacks speed. Serpent algorithm was developed by Ross Anderson, Lars Knudsen and Eli Biham.128-bits block size and key with a length of 128-bits, 192-bits or 256-bits are supported by serpent [30].

Serpent applies a substitution-permutation network to generate the cipher where 32 rounds are needed. Cipher generation is carried out by operating on a block which contains four numbers of 32-bits words. In each round of serpent one of the eight S-boxes are used for 32 times where the size of the each S-box is 4-bit to 4-bit. The algorithm is implemented in such a manner that execution of all the operations can be carried out in parallel.

Same complexity level is present in both for encryption and decryption in serpent scheme. Inverted transformations of the operations which are carried out for encryption are followed in reverse order to perform the decryption. Serpent provides a good level of security though its speed is less. But still, the serpent is faster compared to DES.

3.2.6. Blowfish

Blowfish is block cipher where the symmetric key is applied. Blowfish is designed as a fast alternative algorithm over others in the year 1993 by Bruce Schneier. Good encryption ratio is provided by the blowfish algorithm where full Blowfish shows the ultimate security over hacking. As Blowfish is available in public domain so it is freely accessible.

Block size for Blowfish is 64-bit and variable key length is used for the scheme where the key length varies from 32 bits to 448 bits. Blowfish is Feistel cipher where 16 numbers of rounds are used along with the S-boxes. S-Boxes are dependent on large keys which are generated by Blowfish [98].

As the structure of the Blowfish is simple and numbers of rounds are less so it is very fast cipher though the key schedule is a time consuming operation for Blowfish. Key length for Blowfish is very large and values of the pair of subkeys have changed at generation time. Thus provide great security. As the complexity of the subkey generation is higher due to the running of encryption program 522 times for each key, so security is ultimate that full Blowfish is tense to impossible to hack.

3.2.7. Twofish Algorithm

Twofish is a block cipher where the symmetric key is applied. Twofish is designed as a combination of speed and flexibility in the year 1998. Twofish is derived from other algorithms like Blowfish, SAFER and Square by Bruce Schneier. Free access is possible for Twofish as it is available in the public domain.

Block size of Twofish is 128 bits. The key length of 128-bits, 192-bits or 256-bits is accepted for Twofish. Feistel network structure and 16 numbers of rounds are used for Twofish [57].

Two 32-bit words are considered as input for each round of Twofish and four S-boxes are used where four different keys are present. As additional subkeys are used for XOR operation with the text block before the first round and after last round, thus Twofish is referred to as "prewhitening" and "postwhitening".

The speed of Twofish is very fast and it is flexible for CPU speed, RAM size and hardware configuration of the system. Twofish provides a variety of options and Twofish has a good combination of flexibility, speed and conservative structure.

3.2.8. Chi-Square Test

The chi-Square test is a non-parametric test that defines the magnitude of discrepancy between the data expected from a specific hypothesis and observed data set. The “Chi-square test” is also called as “Pearsonian Chi-square test” or “Chi-squared goodness-of-fit test” [38].

The chi-square test is carried out to decide whether the outcome of encrypted file supposed to be populated from a specified population or not. Higher chi-square value means a specific character having a higher frequency in source file compare to the frequency in the encrypted file.

The chi-Square test is carried out to define the difference between the observed frequencies and the frequencies expected from a specific hypothesis for single or multiple categories. As the total number of distinct classes of possible characters are 256 for source and encrypted files so chi-square test is carried out for 255 (256-1) degrees of freedom.

Some basic conditions that have to be satisfied for chi-square test like independency between observed data, using of original unit of data, random selection of data, number of observations that have to be satisfied for picking a sample and so on.

"Pearsonian Chi-square" is expressed as follows:

$$X^2 = \sum_{i=0}^{n} \frac{(o^i - E^i)^2}{E^i} \quad \text{..... (3.1)}$$

Where

- n stands for total numbers of characters.
- X^2 stands for statistic value for Pearsonian Chi-square test.
- E^i stands for frequency value of i^{th} character in plain text or source file.
- o^i stands for frequency value of i^{th} character in encrypted file.

3.2.9. Degree of Freedom

The degree of freedom for statistical calculation defines the number of values which have the freedom to vary among all the values considered for final calculation. The statistical validity of t-test, chi-square test and f-test are ensured with the help of degree of freedom value [35][95].

Calculation of the degree of freedom depends on the size of samples or observations. Thus if the sample size is large the degree of freedom value is higher and vice versa. The calculation of the degree of freedom is carried out by the following equation

$$DF = (N - 1) \quad \text{.....(3.2)}$$

Where

- DF= Degree of Freedom.
- N= Size of the sample.

3.2.10. Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE)

Peak Signal-to-Noise Ratio (PSNR) [15] represents the ratio between the original signal's possible maximum power and corrupting noise's power which affects the original signal.

PSNR is expressed in decibels and it is considered as the quality measurement between the original image and stego-image. Higher PSNR value indicates the better quality of the compressed image.

Mean Square Error (MSE) is an error metric and it is applied to measure the compression quality of an image. Cumulative squared error is expressed between stego-image and original image by MSE. Lower MSE value is appreciable as it indicates a lower error rate.

Consider an original image a (m, n) and stego-image b (m, n) where b (m, n) is constructed by embedding information bits into it. P and q are representing the number of rows and columns of pixels in the image where m and n are the indexes for rows and columns respectively. The MSE [114] of the encrypted image is calculated by applying the following equation:

$$MSE = \frac{1}{pq}\sum_{0}^{p-1}\sum_{0}^{q-1}[a(m,n) - b(m,n)]^2 \quad \text{..... (3.3)}$$

PSNR is calculated by using following equation:

$$\text{PSNR} = 10.\log_{10}\left[\frac{\text{MAX}_m^2}{\text{MSE}}\right] \quad \text{..... (3.4)}$$
$$= 20.\log_{10}\left[\frac{\text{MAX}_m}{\sqrt{\text{MSE}}}\right]$$

Where MAX_m represents the maximum possible value of the pixel of image. The value is 255 when pixels are represented in 8 bits per sample.

3.2.11. Structural Similarity Index Metric (SSIM)

The similarity between two images is accessed by applying the method of Structural Similarity Index Metric (SSIM) [79]. The perceptual difference between the two images

is measured by SSIM. Image quality degradation due to data compression or data transmission is quantified by SSIM. When the pixels of the image are spatially close then strong inter-dependencies is present between them. Important information is carried out regarding the structure of the image in a visual scene based on the inter-dependencies of the pixels. SSIM is implemented to improve the existing procedures such as Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) which are considered to be inconsistent for human visual perception.

Various windows from an image can be considered for calculating the SSIM index. SSIM index is calculated between two windows p and q with a common size M×M by applying the following equation:

$$SSIM\ (p,q) = \frac{(2\mu_p\mu_q + c_1)(2\sigma_{pq} + c_2)}{(\mu_p^2 + \mu_q^2 + c_1)(\sigma_p^2 + \sigma_q^2 + c_2)} \quad \text{..... (3.5)}$$

Where

- μ_p stands for average value of p.
- μ_q stands for average value of q.
- σ_p^2 stands for variance of p.
- σ_q^2 stands for variance of q.
- σ_{pq} stands for co-variance of p and q.
- $C_1 = (k_1 L)^2$ and $C_2 = (k_2 L)^2$ are the two variable values for stabilizing the division with very weak denominator where default values of k_1 is 0.01 and k_2 is 0.03.
- L stands for the dynamic range of pixel values.

3.2.12. Universal Image Quality Index

Universal Image Quality Index [79] is applied to measure the distortion of image and video. Three factors namely correlation loss, luminance distortion and distortion of contrast are combined together to represent the Universal Image Quality Index. Image

distortion in respect of reference image is modelled to define the quality index. The Universal Quality Index (Q) is calculated in respect of the following equations:

$$Q = \frac{\sigma_{fg}}{\sigma_f \cdot \sigma_g} \cdot \frac{2\,\overline{f}\,\overline{g}}{\left(\overline{f}\right)^2 + \left(\overline{g}\right)^2} \cdot \frac{2\,\sigma_f \cdot \sigma_g}{\sigma_f^{\,2} + \sigma_g^{\,2}} \quad \text{..... (3.6)}$$

Where

$$\overline{f} = \frac{1}{MN} \sum_{p=0}^{R-1} \sum_{q=0}^{S-1} OI \quad ; \qquad \overline{g} = \frac{1}{MN} \sum_{p=0}^{R-1} \sum_{q=0}^{S-1} EI \quad ;$$

$$\sigma_{fg} = \frac{1}{M+N-1} \sum_{p=0}^{R-1} \sum_{q=0}^{S-1} [OI - \overline{f}][EI - \overline{g}] \; ; \qquad \sigma_f^{\,2} = \frac{1}{M+N-1} \sum_{p=0}^{R-1} \sum_{q=0}^{S-1} [OI - \overline{f}]^2 \; ;$$

$$\sigma_g^{\,2} = \frac{1}{M+N-1} \sum_{p=0}^{R-1} \sum_{q=0}^{S-1} [EI - \overline{g}]^2 \; ;$$

Where

- *OI* and *EI* stand for the original image and stego image with the size of ($R \times S$) containing the pixels values f(p, q) and g(p, q) for the original image and stego image respectively where ($0 \geq p > R$, $0 \geq q > S$).

The first component is applied to measure the correlation coefficient of the two images. The second component performs the calculations regarding luminance between images whose range is [0, 1]. The third component is responsible to access the similarity of contrast of two images where the range is in between [0, 1]. The range of Universal Image Quality Index is [-1, 1] where two images are totally identical when the range value is 1.

3.2.13. Bit Error Rate (BER)

Bit Error Rate (BER) [54][62] is defined as a percentage of numbers of corrupted bits relative to total numbers of bits present in the cover image. BER is represented with

respect to a negative power of ten. The Bit Error Rate (BER) is calculated in respect of the following equation:

$$BER = \frac{CB}{TB} \quad \text{..... (3.7)}$$

Where

- *CB* stands for total numbers of bits which are corrupted.
- *TB* stands for total numbers of bits present in the cover image.

3.2.14. Correlation Coefficient (CC)

Correlation Coefficient [36] accesses the degree of strength of the statistical relationship between two variables. It is a statistical measure where a variable may be columns of observations or components of multivariate random values. Different types of correlation coefficient are presents where their definition, usability and characteristic vary depending upon its type.

The most common and widely used correlation coefficient is the Pearson product-moment correlation coefficient which is developed by Karl Pearson. Strength and direction of the linear relationship of two variables M and N are measured by the Pearson correlation coefficient. The range of Correlation Coefficient is bounded by -1 to +1 where total positive correlation and total negative correlation are represented by +1 and -1 respectively and 0 represents no correlation between the variables. Correlation coefficient (ρ) value is calculated by using the following formula:

$$\rho M, N = \frac{\text{cov}(M, N)}{\sigma_M \sigma_N} = \frac{E[(M - \mu_M)(N - \mu_N)]}{\sigma_M \sigma_N} \quad \text{..... (3.8)}$$

Where

- **C**ov stands for co-variance.
- σ_M and σ_N stand for standard deviation of *M* and *N* respectively.
- μ_M and μ_N stand for mean of *M* and *N* respectively.
- E stands for expectation.

3.2.15. Normalized Cross-Correlation (NCC)

Normalized Cross-Correlation (NCC) defines the closeness between two images. Correlation functions can be applied to measure the closeness of digital images. The similarity between images is measured by Normalized Cross-Correlation [120] with the help of the following equations:

$$NCC = \frac{\sum_{p=1}^{R} \sum_{q=1}^{C} (OI \times EI)}{\sum_{P=1}^{R} \sum_{q=1}^{C} |OI|^2} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(3.9)}$$

Where

- R and C stand for numbers of rows and numbers of columns respectively.
- OI and EI stand for original image and corresponding stego-image respectively.

3.3. Conclusion

In this chapter, the issues and the parameters related to the performance assessment for implemented schemes are discussed. Performance metrics have been assessed in terms of security measurement over different attacks for the user authentication system. For encryption system, performance metrics have been measured in respect of hypothetical distribution. The degree of freedom, chi-square test and other metrics are considered for assessing the performance of text encryption schemes whereas PSNR, SSIM, Q-INDEX, Correlation Coefficient, NCC and other metrics are applied to measure the performance of image encryption schemes.