A Study on Statistical Analysis and Security Evaluation Parameters in Image Encryption

Dr. Kalyani Mali[1] Shouvik Chakraborty[2] Mousomi Roy[3]
[1,2,3]Department of Computer Science & Engineering
[1,2,3]University of Kalyani West Bengal, 741235, India

Abstract— In recent years, a significant improvement in multimedia technologies has been observed and therefore, transmission of these data over the network is very common. The network (mainly internet) is not a secure channel and it has a number of security related problems. To achieve security of multimedia data over an insecure channel, a number of encryption methods have been developed. This paper gives a study on different methodology to evaluate image encryption techniques proposed in the literature. Only the visual inspection is not enough and therefore a number of parameters like, correlation coefficient, NPCR. UACI, information entropy, compression friendliness, PSNR, histogram analysis etc., are used, to judge the quality of encrypted images.

Key words: Image Encryption, Cryptosystem

I. INTRODUCTION

The transmission of multimedia contents over insecure networks has several security problems. As a result, multimedia data security has become a serious and major issue in telemedicine, , financial transaction and mobile phone applications etc. [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 type 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.

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 [5].

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].

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 require long computational time and high computing power [23]–[25].

II. EVALUATION PARAMETERS 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]. Mathematically correlation coefficient can be written using (2.1) [28]–[30].

$$R_{xy} = COV(xy) / \sqrt{D(x)}\sqrt{D(y)} \tag{2.1}$$

Where,

$$COV(xy)\frac{1}{T}\sum_{i=1}^{T}((x_i - E(x))(y_i - E(y))) \tag{2.2}$$

$$E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i , E(y) = \frac{1}{T}\sum_{j=1}^{T} y_j \tag{2.3}$$

$$D(x) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x_i))^2 , D(y) = \frac{1}{T}\sum_{j=1}^{T}(y_j - E(y_j))^2 \tag{2.4}$$

B. Information Entropy Analysis

Entropy of a source gives idea about self-information i.e., information provided by a random process about itself [31].

All rights reserved by www.ijsrd.com

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 of an image is calculated using (2.5).

$$H(s) = -\sum_{i=0}^{N-1} p(s_i) \log_2 p(s_i) \qquad (2.5)$$

Where $p(s_i)$ is the possibility of presence of the symbol s_i. The entropy of an image shows the distribution of the gray scale values. Higher entropy information is obtained in more uniform distributions.

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 methods impact data compressibility or generate 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]:

- Calculate the histogram of the plaintext image and the cipher text image.
- Let d be the absolute difference between the two histograms obtained in Step 1.
- Let d_i be the amplitude of histogram at index i, then the sum of deviation can be calculated using (2.6) [28].

$$D = \frac{d_0 + d_{255}}{2} + \sum_{i=1}^{254} d_i \qquad (2.6)$$

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 (6) the sum of deviation between plaintext image and cipher text 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 situation 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:

- Take the absolute difference of plaintext, *P* image and the cipher text, *C* image [30].

$$D = |P - C| \qquad (2.7)$$

- Calculate the histogram of *D*.

$$H = histogram(D) \qquad (2.8)$$

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

$$M_H = \frac{1}{256} \sum_{i=0}^{255} h_i \qquad (2.9)$$

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

$$H_{D_i} = |h_i - M_H| \qquad (2.10)$$

- Now irregular deviation I_D is calculated as follows [30].

$$I_D = \sum_{i=0}^{255} H_{D_i} \qquad (2.11)$$

Smaller the value of I_D, better the encryption quality. Using (11) 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

All rights reserved by www.ijsrd.com

proposed that describes a formula for deviation from an ideal assumed uniform histogram [38]. Let H_C be the histogram of the cipher text image and let H_{Ci} be the value of the frequency of occurrence at index i, then uniform histogram is represented as [38]:

$$H_{C_i} = \frac{MXN}{256} \quad 0 \le C_i \le 255 \qquad (2.12)$$
$$= 0 \quad elsewhere$$

The deviation from uniform histogram shown by (12) is calculated as [38]:

$$D_p = \frac{\sum_{C_i=0}^{255} H_{C_i} - H_c}{MXN} \qquad (2.13)$$

The lower value of D_P represents better encryption quality because the lower value indicates that the histogram of cipertext image is less deviated from uniform histogram and can be measured by (13).

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 cipher text image [19]. Mathematically [19]:

$$PSNR = 10\log_{10}\left(\frac{L^2}{MSE}\right) \qquad (2.14)$$

Where

$$MSE = \frac{1}{N}\sum_{i=0,j=0}^{N,N}(x_{ij} - y_{ij})^2 \qquad (2.15)$$

N is the number of pixels in the frame, and x_{ij}, y_{ij} is the i^{th} and j^{th} pixels in the original and processed frames, respectively. L is the dynamic range of pixel values (L is 0 to 255 for gray-scale images).

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 cipher text should change completely, in an unpredictable manner. Diffusion characteristics of an image encryption algorithm mean that the output pixels of cipher text 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 cipher text 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 cipher text image. Mean Square Error (MSE) is the cumulative squared error between two digital images and can be used to check the avalanche effect. MSE can be calculated using (2.15) [20], [21].

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 cipher text 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], [20], [22], [26]. NPCR and UACI can be defined using (2.16) and (2.17) respectively [23].

$$NPCR = \frac{\sum_{i=1,j=1}^{m,n} D(i,j)}{w\,X\,h} X100\% \qquad (2.16)$$

$$UACI = \frac{1}{w\,X\,h}\left[\sum_{i,j}^{m,n}\frac{|C_1(i,j) - C_2(i,j)|}{255}\right] X100\% \qquad (2.17)$$

Where C_1 and C_2 are two encrypted images corresponding to two original images with subtle change i.e., one pixel difference. w and h are the image width and height , D(i, j) is a bipolar array with the same size as image C_1 ,$D(i, j)$ is determined using on (2.18).

$$D(i,j) = 1 if\ C_1(i,j) = C_2(i,j) \qquad (2.18)$$
$$= 0 otherwise$$

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 [15]. Key space analysis is summarized in the following Section [15].

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], [15]. 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 2k 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. 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 cipher text image correctly, even if there is a one bit difference between key [16]. 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 [16].

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

All rights reserved by www.ijsrd.com

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 [39], [17]. To find a weakness in cipher text, 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 [39], [17].

1) Cipher text only Attack:

In this type of attack, the cryptanalyst has access to a set of cipher text. In cipher text only attack, encryption algorithm and cipher text 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 cipher text [3], [39], [17]. 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 cipher text 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 cipher text. 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 Cipher text Only Attack:

The attacker can choose cipher text and get the corresponding plaintext. By selecting some cipher text a cryptanalyst has access to corresponding decrypted plaintext. Chosen cipher text only attack is more applicable to public key cryptosystems [3].

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 [4], [13].

III. Conclusion

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. These methods are very effective and can be implemented for testing cryptographic algorithms.

References

[1] B. Acharya, S. Patra, and G. Panda, "Image encryption by novel cryptosystem using matrix transformation," in Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on. IEEE, 2008, pp. 77–81.

[2] G. Jakimoski and K. Subbalakshmi, "Cryptanalysis of some multimedia encryption schemes," Multimedia, IEEE Transactions on, vol. 10, no. 3, pp. 330–338, 2008.

[3] B. Schneier, Applied Cryptography. John Wiley & Sons, Inc., USA, 1996.

[4] W. Stallings, Cryptography and network security: principles and practice. Prentice Hall, 2010, vol. 998.

[5] B. Furht and D. Socek, "a survey of multimedia security," Comprehensive Report on, 2003.

[6] D. Van De Ville, W. Philips, R. Van de Walle, and I. Lemahieu, "Image scrambling without bandwidth expansion," Circuits and Systems for Video Technology, IEEE Transactions on, vol. 14, no. 6, pp. 892–897, 2004.

[7] Y. Chen and L. Chang, "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. IEEE, 2001, pp. 518–521.

[8] R. Chandramouli, N. Memon, and M. Rabbani, "Digital watermarking," Encyclopedia of Imaging Science and Technology, 2002.

[9] M. Holliman and N. Memon, "Counterfeiting attacks on oblivious blockwise independent invisible watermarking schemes," Image Processing, IEEE Transactions on, vol. 9, no. 3, pp. 432–441, 2000.

[10] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," Signal processing, vol. 66, no. 3, pp. 283–301, 1998.

[11] ——, "Digital watermarking of raw and compressed video," in Proc. European EOS/SPIE Symposium on Advanced Imaging and Network Technologies, vol. 2952. Citeseer, 1996, pp. 205–213.

[12] B. Furht and D. Kirovski, Multimedia security handbook. CRC, 2005, vol. 4.

[13] C. Li, S. Li, D. Zhang, and G. Chen, "Cryptanalysis of a data security protection scheme for voip," in Vision, Image and Signal Processing, IEE Proceedings-, vol. 153, no. 1. IET, 2006, pp. 1–10.

[14] Y. Mao and G. Chen, "Chaos-based image encryption," Handbook of Geometric Computing, pp. 231–265, 2005.

[15] L. Chuanmu and H. Lianxi, "A new image encryption scheme based on hyperchaotic sequences," in Anti-counterfeiting, Security, Identification, 2007 IEEE International Workshop on. IEEE, 2007, pp. 237–240.

[16] H. Liu, Z. Zhu, H. Jiang, and B. Wang, "A novel image encryption algorithm based on improved 3d chaotic cat map," in Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for. IEEE, 2008, pp. 3016–3021.

[17] J. Zhou, O. Au, X. Fan, and P. Wong, "Joint security and performance enhancement for secure arithmetic coding," in Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on. IEEE, 2008, pp. 3120–3123.

[18] S. Lian, Multimedia content encryption: techniques and applications. Auerbach Publications, 2008.

[19] M. El-lskandarani, S. Darwish, and S. Abuguba, "A robust and secure scheme for image transmission over wireless channels," in Security Technology, 2008.

All rights reserved by *www.ijsrd.com*

ICCST 2008. 42nd Annual IEEE International Carnahan Conference on. IEEE, 2008, pp. 51–55.
[20] A. Mohamed, G. Zaibi, and A. Kachouri, "Implementation of rc5 and rc6 block ciphers on digital images," in Systems, Signals and Devices (SSD), 2011 8th International Multi-Conference on. IEEE, 2011, pp. 1–6.
[21] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Securing information content using new encryption method and steganography," in Digital Information Management, 2008. ICDIM 2008. Third International Conference on. IEEE, 2008, pp. 563–568.
[22] I. Ismail, M. Amin, and H. Diab, "A digital image encryption algorithm based a composition of two chaotic logistic maps," International Journal of Network Security, vol. 11, no. 1, pp. 1–10, 2010.
[23] T. Dan andW. Xiaojing, "Image encryption based on bivariate polynomials," in Computer Science and Software Engineering, 2008 International Conference on, vol. 6. IEEE, 2008, pp. 193–196.
[24] H. Ahmed, H. Kalash, and O. Allah, "Encryption efficiency analysis and security evaluation of rc6 block cipher for digital images," in Electrical Engineering, 2007. ICEE'07. International Conference on. IEEE, 2007, pp. 1–7.
[25] N. Flayh, R. Parveen, and S. Ahson, "Wavelet based partial image encryption," in Multimedia, Signal Processing and Communication Technologies, 2009. IMPACT'09. International. IEEE, 2009, pp. 32–35.
[26] H. Nien, S. Changchien, S. Wu, and C. Huang, "A new pixel-chaoticshuffle method for image encryption," in Control, Automation, Robotics and Vision, 2008. ICARCV 2008. 10th International Conference on. IEEE, 2008, pp. 883–887.
[27] I. Elashry, O. Allah, A. Abbas, S. El-Rabaie, and F. El-Samie, "Homomorphic image encryption," Journal of Electronic Imaging, vol. 18, p. 033002, 2009.
[28] N. El-Fishawy and O. Zaid, "Quality of encryption measurement of bitmap images with rc6, mrc6, and rijndael block cipher algorithms," International Journal of Network Security, vol. 5, no. 3, pp. 241–251, 2007.
[29] S. Kamali, R. Shakerian, M. Hedayati, and M. Rahmani, "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. IEEE, 2010, pp. V1–141.
[30] H. Elkamchouchi and M. Makar, "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. IEEE, 2005, pp. 277–284.
[31] R. Gray, Entropy and information theory. Springer Verlag, 2010.
[32] X. Shu-Jiang, W. Ying-Long, W. Ji-Zhi, and T. Min, "A novel image encryption scheme based on chaotic maps," in Signal Processing, 2008. ICSP 2008. 9th International Conference on. IEEE, 2008, pp. 1014–1018.
[33] C. Shannon, "Communication theory of secrecy systems," Bell system technical journal, vol. 28, no. 4, pp. 656–715, 1949.
[34] H. Ahmed, H. Kalash, and O. Allah, "Implementation of rc5 block cipher algorithm for image cryptosystems," International Journal of Information Technology, vol. 3, no. 4.
[35] R. Enayatifar, "Image encryption via logistic map function and heap tree," Int. J. Phys. Sci, vol. 6, no. 2, p. 221, 2011.
[36] Z. Han, W. Feng, L. Hui, L. Da Hai, and L. Chou, "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. IEEE, 2003, pp. 778–782.
[37] J. Shah and V. Saxena, "Performance study on image encryption schemes," International Journal of Computer Science, vol. 8.
[38] I. E. Elashry, "Digital image encryption," MS Thesis, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menofia University, 2010.
[39] W. Zeng, H. Yu, and C. Lin, Multimedia security technologies for digital rights management. Academic Pr, 2006.

All rights reserved by www.ijsrd.com