ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Cryptanalysis of Digital Imaging and Communications in Medicine (DICOM) Medical contents Encryption using Modified Vigenere Cipher and Multilevel Encryption Methodologies.

P Subhasri*, and A Padmapriya.

Department of Computer Science, Alagappa University – Karaikudi

ABSTRACT

In healthcare management systems, the security of medical details are the essential, because the patient's particulars can be identified using these details. Basically, cryptographic schemes are used to enhance the security and confidentiality of medical details during communications. Therefore a standard is needed to preserve the medical details. Digital Imaging and Communications in Medicine (DICOM) is the universal standard for communication in medical contents. In cryptographic technique, after the encryption process, intruders may hack the sensitive data without using precise key and is known as cryptanalysis. So a typical evaluation mechanism is needed to verify the cryptographic methods quality. In this paper, an effective new of two mechanisms namely modified vigenere cipher and multilevel encryption methodologies used to enhance the security of DICOM medical contents. The performance analyses of these two methodologies are evaluated by various quality measures. In addition, the cryptanalysis is also performed to measure the strength of these methods.

Keywords: DICOM Medical contents, Cryptography, Cryptanalysis, Quality measures, Security attacks.

**Corresponding author*

INTRODUCTION

The advanced developments of communication technologies provide a significant improvement in the field of the medical records management system. The medical records contain the patient details and reports are most commonly represented as images that are to be confidentially maintained. The patient health records contain sensitive particulars so it is a leading challenge to share these data over the network [2]. The intruders may hack these confidential matters or modify that, which may lead to wrong treatment for the patient. At this point, the integrity and privacy is essential to validate the sensitive medical details [12].

The DICOM (Digital Imaging and Communication in Medicine) has been the universal standard for secured communications of medical images over networks [2]. It was invented by National Electrical Manufacturers Association (NEMA) in 1983. It contains four security profiles namely; secure usage profiles, secure transport connection profiles, digital signature profiles, and media storage security profiles to confirm whether the health records are protected during its transmission. For sending the medical records among different departments within hospital campus and other hospitals, the DICOM technology is more suitable [3].

The paper is organized as follows. Section 1 provides a general description of security in medical images using DICOM details. Section 2 presents a brief study of the background work. Section 3 elaborates the methodology considered for cryptanalysis namely, modified vigenere cipher method, and multilevel encryption methodology. Section 4 contains the performance analysis of the methodologies elaborated in section 3. Section 5 includes the information about cryptanalysis and its attacks. The efficiency and contributions of this paper are concluded in section 6.

BACKGROUND STUDY

Encryption is the vital and valuable methodology to assure the security for the period of DICOM communications [4]. Cryptography will modify the original contents into the in-comprehensible format and sends the information over an unprotected channel. The authorized person has the ability to convert the non-readable information to readable one. There are two techniques namely [4] transposition and substitution for converting the medical details into the non readable form. In transposition cipher, the encryption process is performed by the positions held by units of plaintext are transferred according to a usual system or pattern, so that the cipher text composes a transformation of the plaintext [12]. A substitution cipher is a process of encoding by which units of plaintext are replaced with the cipher text. Cryptanalysis is a major part of modern cryptology and focuses on the security analysis of different kinds of cryptographic algorithms. The performance of the various cryptographic algorithms quality is evaluated by the cryptanalysis attacks.

DICOM is used in radiology, cardiology, radiotherapy, oncology, ophthalmology, dentistry, and so on. It is a standard technology processed virtually in hospitals, imaging centers, and experts. DICOM is an object which was described by attributes [3]. DICOM objects are standardized according to Information Object Definitions (IOD). An IOD is a group of attributes relating a data object these are listed in the DICOM Data Dictionary. The attributes involved various data types for its accurate representation. DICOM image file format stores the details of the image and integral part of the patient record in the same file [3]. For example, consider a Knee CT image it actually contains the details about the patient within the file.

METHODOLOGIES CONSIDERED FOR CRYPTANALYSIS

Enhancing the Security of DICOM Content using Modified Vigenere Cipher

An efficient mechanism is used to enhance the security of Dicom content using modified Vigenere cipher [8]. In this method, the Dicom file is split into watermarked Bmp image and tag. Both portions are encrypted by modified vigenere cipher technique. Basically, a normal vigenere cipher technique contains 0-25 possible numbers to encode original content. In modified vigenere cipher technique, 0-255 numbers are generated randomly throughout the processing. The modified vigenere table consists of the numbers written out 256 times in different rows, each number shifted cyclically to the left compared to the previous number, corresponding to the 256 possible numbers [8]. The size of the key generated depends upon the size of the input.

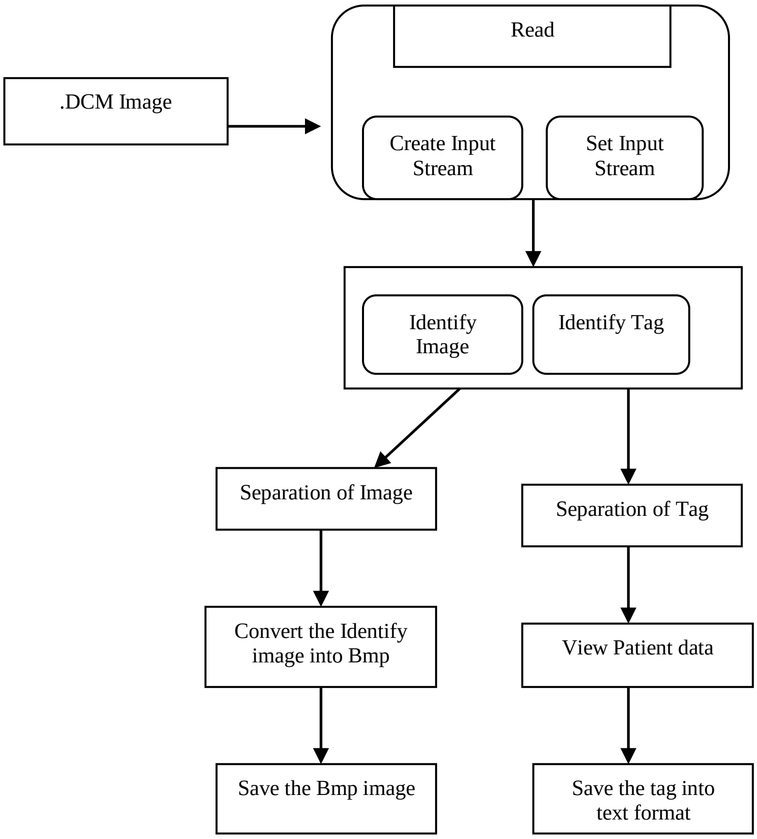


Figure 1: Architecture Design of Modified Vigenere Cipher Technique

Multilevel Encryption Methodology for Securing DICOM Content

In Multilevel encryption methodology [9] there are three levels of encryptions such as i) Position based transposition, ii) XOR and iii) Advanced Vigenere cipher substitution are used to secured the DICOM content. The image and tag are given as input and the key was generated depend upon the size of input image/tag. Suppose the input size is 256 x 256, the key generated will also be of 256 x 256. Then the input is positional transposed by the key. Position based transposition is the key based transposition which the input matrix are defined by positions in ascending order. The input matrix is replaced by the key matrix depends upon its positions to get the ciphered matrix. And then apply XOR operation, the resultant matrix value is taken as row index and key value taken as the column index. Apply substitution using the advanced Vigenere cipher table. This Vigenere cipher table row is changed in every time during the image ordered is odd and even [9].

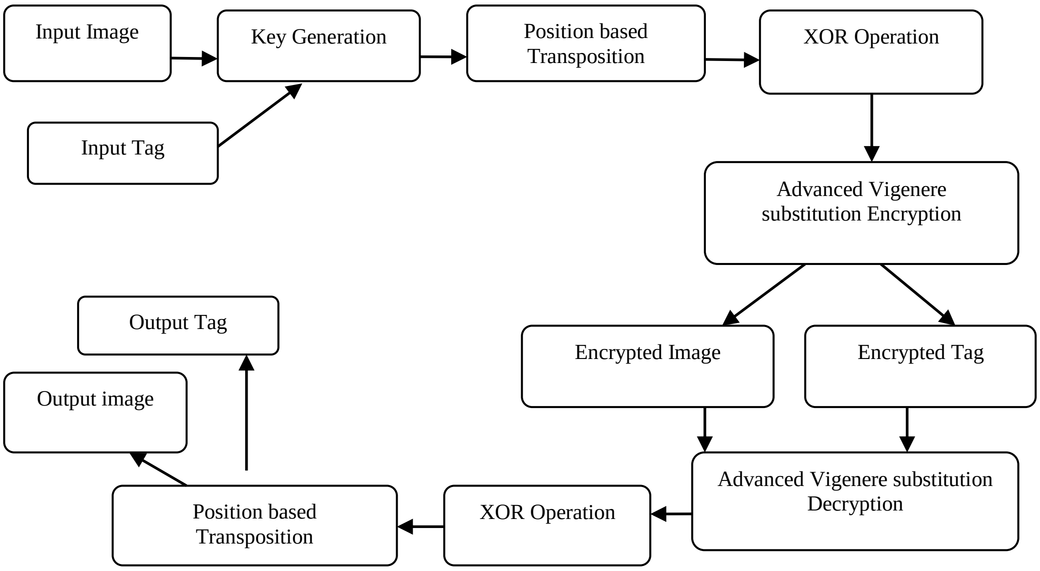
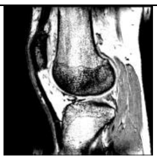
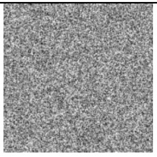
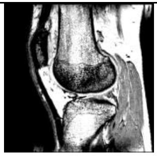
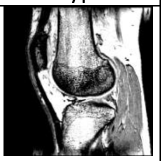
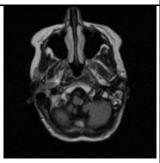
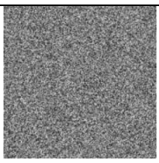
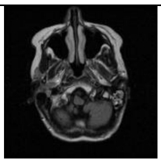
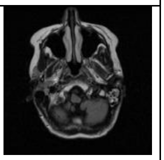
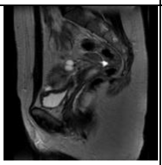
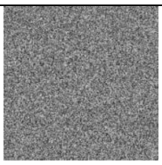
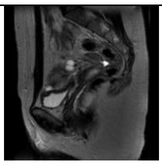
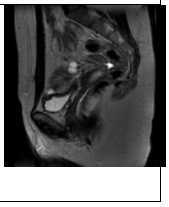
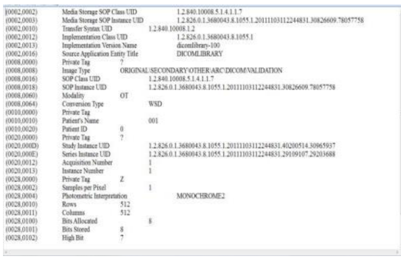

Input Image
Key Generation
Position based Transposition
XOR Operation
Input Tag
Advanced Vigenere substitution Encryption
Output Tag
Encrypted Image
Encrypted Tag
Output image
Advanced Vigenere substitution Decryption
Position based Transposition
XOR Operation

Figure 2: Overall process for DICOM Content Encryption/Decryption

Bmp DICOM Image Encryption/Decryption using Modified Vigenere Cipher and Multilevel Encryption Method

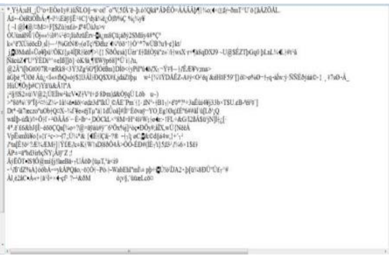
	Original Image	Modified Vigenere cipher		Multilevel Encryption Method	
		Encrypted	Decrypted	Encrypted	Decrypted
Image 1 Knee, MR Image					
Image 2 Head, CT Image					
Image 3 Ankle, X-Ray Image					

DICOM Tag Encryption/Decryption using Modified Vigenere Cipher Method



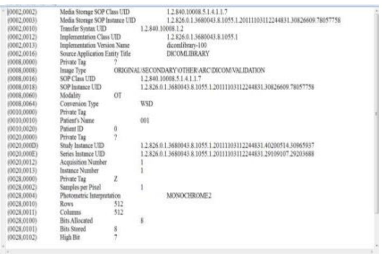
```
(0002,0002)   Media Storage SOP Class UID          1.2.840.10008.5.1.4.1.1.7
(0002,0003)   Media Storage SOP Instance UID       1.2.826.0.1.3680043.8.1055.1.20111103112244831.30826609.78057758
(0002,0010)   Transfer Syntax UID        1.2.840.10008.1.2
(0002,0012)   Implementation Class UID             1.2.826.0.1.3680043.8.1055.1
(0002,0013)   Implementation Version Name          dicomlibrary-100
(0002,0016)   Source Application Entity Title      DICOMLIBRARY
(0008,0000)   Private Tag       ?
(0008,0008)   Image Type        ORIGINAL\SECONDARY\OTHER\ARC\DICOM\VALIDATION
(0008,0016)   SOP Class UID              1.2.840.10008.5.1.4.1.1.7
(0008,0018)   SOP Instance UID           1.2.826.0.1.3680043.8.1055.1.20111103112244831.30826609.78057758
(0008,0060)   Modality          OT
(0008,0064)   Conversion Type            WSD
(0010,0000)   Private Tag
(0010,0010)   Patient's Name             001
(0010,0020)   Patient ID        0
(0020,0000)   Private Tag       ?
(0020,000D)   Study Instance UID         1.2.826.0.1.3680043.8.1055.1.20111103112244831.40200514.30965937
(0020,000E)   Series Instance UID        1.2.826.0.1.3680043.8.1055.1.20111103112244831.29109107.29203688
(0020,0012)   Acquisition Number         1
(0020,0013)   Instance Number            1
(0028,0000)   Private Tag       Z
(0028,0002)   Samples per Pixel          1
(0028,0004)   Photometric Interpretation           MONOCHROME2
(0028,0010)   Rows              512
(0028,0011)   Columns           512
(0028,0100)   Bits Allocated             8
(0028,0101)   Bits Stored       8
(0028,0102)   High Bit          7
```

Input Tag



[illegible]

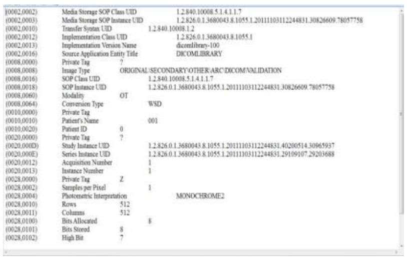
Encrypted Tag



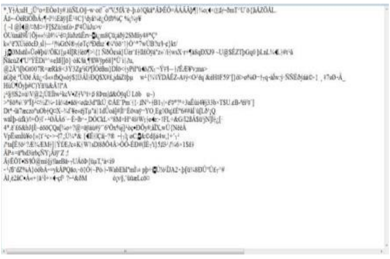
```
(0002,0002)   Media Storage SOP Class UID          1.2.840.10008.5.1.4.1.1.7
(0002,0003)   Media Storage SOP Instance UID       1.2.826.0.1.3680043.8.1055.1.20111103112244831.30826609.78057758
(0002,0010)   Transfer Syntax UID        1.2.840.10008.1.2
(0002,0012)   Implementation Class UID             1.2.826.0.1.3680043.8.1055.1
(0002,0013)   Implementation Version Name          dicomlibrary-100
(0002,0016)   Source Application Entity Title      DICOMLIBRARY
(0008,0000)   Private Tag       ?
(0008,0008)   Image Type        ORIGINAL\SECONDARY\OTHER\ARC\DICOM\VALIDATION
(0008,0016)   SOP Class UID              1.2.840.10008.5.1.4.1.1.7
(0008,0018)   SOP Instance UID           1.2.826.0.1.3680043.8.1055.1.20111103112244831.30826609.78057758
(0008,0060)   Modality          OT
(0008,0064)   Conversion Type            WSD
(0010,0000)   Private Tag
(0010,0010)   Patient's Name             001
(0010,0020)   Patient ID        0
(0020,0000)   Private Tag       ?
(0020,000D)   Study Instance UID         1.2.826.0.1.3680043.8.1055.1.20111103112244831.40200514.30965937
(0020,000E)   Series Instance UID        1.2.826.0.1.3680043.8.1055.1.20111103112244831.29109107.29203688
(0020,0012)   Acquisition Number         1
(0020,0013)   Instance Number            1
(0028,0000)   Private Tag       Z
(0028,0002)   Samples per Pixel          1
(0028,0004)   Photometric Interpretation           MONOCHROME2
(0028,0010)   Rows              512
(0028,0011)   Columns           512
(0028,0100)   Bits Allocated             8
(0028,0101)   Bits Stored       8
(0028,0102)   High Bit          7
```

Decrypted Tag

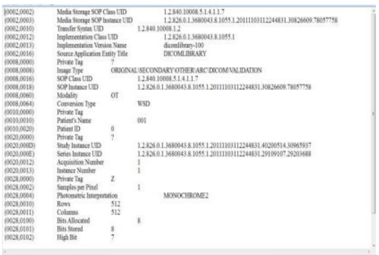
DICOM Tag Encryption/Decryption using Multilevel Encryption Method



```
(0002,0002)   Media Storage SOP Class UID              1.2.840.10008.5.1.4.1.1.7
(0002,0003)   Media Storage SOP Instance UID           1.2.826.0.1.3680043.8.1055.1.20111103112244831.30826609.78057758
(0002,0010)   Transfer Syntax UID            1.2.840.10008.1.2
(0002,0012)   Implementation Class UID                 1.2.826.0.1.3680043.8.1055.1
(0002,0013)   Implementation Version Name              dicomlibrary-100
(0002,0016)   Source Application Entity Title          DICOMLIBRARY
(0008,0000)   Private Tag          ?
(0008,0008)   Image Type           ORIGINAL\SECONDARY\OTHER\ARC\DICOM\VALIDATION
(0008,0016)   SOP Class UID                  1.2.840.10008.5.1.4.1.1.7
(0008,0018)   SOP Instance UID               1.2.826.0.1.3680043.8.1055.1.20111103112244831.30826609.78057758
(0008,0060)   Modality             OT
(0008,0064)   Conversion Type                WSD
(0010,0000)   Private Tag
(0010,0010)   Patient's Name                 001
(0010,0020)   Patient ID           0
(0020,0000)   Private Tag          ?
(0020,000D)   Study Instance UID             1.2.826.0.1.3680043.8.1055.1.20111103112244831.40200514.30965937
(0020,000E)   Series Instance UID            1.2.826.0.1.3680043.8.1055.1.20111103112244831.29109107.29203688
(0020,0012)   Acquisition Number             1
(0020,0013)   Instance Number                1
(0028,0000)   Private Tag          Z
(0028,0002)   Samples per Pixel              1
(0028,0004)   Photometric Interpretation               MONOCHROME2
(0028,0010)   Rows                 512
(0028,0011)   Columns              512
(0028,0100)   Bits Allocated                 8
(0028,0101)   Bits Stored          8
(0028,0102)   High Bit             7
```



```
[illegible]
```



```
(0002,0002)   Media Storage SOP Class UID              1.2.840.10008.5.1.4.1.1.7
(0002,0003)   Media Storage SOP Instance UID           1.2.826.0.1.3680043.8.1055.1.20111103112244831.30826609.78057758
(0002,0010)   Transfer Syntax UID            1.2.840.10008.1.2
(0002,0012)   Implementation Class UID                 1.2.826.0.1.3680043.8.1055.1
(0002,0013)   Implementation Version Name              dicomlibrary-100
(0002,0016)   Source Application Entity Title          DICOMLIBRARY
(0008,0000)   Private Tag          ?
(0008,0008)   Image Type           ORIGINAL\SECONDARY\OTHER\ARC\DICOM\VALIDATION
(0008,0016)   SOP Class UID                  1.2.840.10008.5.1.4.1.1.7
(0008,0018)   SOP Instance UID               1.2.826.0.1.3680043.8.1055.1.20111103112244831.30826609.78057758
(0008,0060)   Modality             OT
(0008,0064)   Conversion Type                WSD
(0010,0000)   Private Tag
(0010,0010)   Patient's Name                 001
(0010,0020)   Patient ID           0
(0020,0000)   Private Tag          ?
(0020,000D)   Study Instance UID             1.2.826.0.1.3680043.8.1055.1.20111103112244831.40200514.30965937
(0020,000E)   Series Instance UID            1.2.826.0.1.3680043.8.1055.1.20111103112244831.29109107.29203688
(0020,0012)   Acquisition Number             1
(0020,0013)   Instance Number                1
(0028,0000)   Private Tag          Z
(0028,0002)   Samples per Pixel              1
(0028,0004)   Photometric Interpretation               MONOCHROME2
(0028,0010)   Rows                 512
(0028,0011)   Columns              512
(0028,0100)   Bits Allocated                 8
(0028,0101)   Bits Stored          8
(0028,0102)   High Bit             7
```

Input Tag Encrypted Tag Decrypted Tag

PERFORMANCE ANALYSIS

Quality measures

An image processing system has a number of distortion or artifacts, so the quality measure is the significant one to be considered [10]. There are several metrics and parameters that can be used to evaluate the quality of the image. They are classified as Full Reference (FR) and No Reference (NR) methods [10]. In FR method the test image quality is assessed by comparing a reference image which is assumed to have perfect excellence. NR method assesses the test image eminence without any reference to the original one. In this paper, the quality measures of the modified vigenere cipher and multilevel encryption technique are tested with 3 various types of DICOM watermarked images by through FR process. The observations reveal that the [9&10] method is more secured. The parameters [10] considered for image quality analysis are given below,

Peak Signal-to-Noise Ratio (PSNR)

PSNR value characterizes the quality of the original image with encrypted image. When the PSNR value is low, it confirmed the encryption quality is enhanced.

$$\text{PSNR}= 10 \log \frac{(2^{n}-1)}{MSE} = 10\log\frac{255^{2}}{MSE}$$

Number of Pixels Changing Rate (NPCR)

Number of Pixels Change Rate (NPCR) stands for the number of pixels change rate while, one pixel of plain image is changed.

$$\text{NPCR}= \frac{\sum_{(\ i,j\ )} D(i,j)}{W*H}*100\%$$

Unified Average Changing Intensity (UACI)

It measures the average intensity of differences between the plain image and ciphered image.

$$\text{UACI}= \frac{1}{W*H}\left[\sum_{i,j}\frac{C1(i,j)-C2(i,j)}{255}\right]*100\%$$

Correlation Coefficient (CC)

Correlation coefficient assesses the correlation between two adjoining pixels in an image. Generally, correlation measures the degree of similarity between two pixels.

$$\text{Cov (x,y)} = \frac{1}{N}\sum_{i=1}^{N}(xi-E(x))(yi-(E(y))$$

Performance Analysis

Table 1: Performance and Comparative Analysis of Modified Vigenere Cipher and Multilevel Encryption Technique with Existing Methods

Quality Parameters	Enhancement of AES algorithm based on chaotic maps and shift operation for image encryption [11]			An image encryption scheme based on hybrid orbit of hyper chaotic systems [10]			**Modified Vigenere Cipher**			**Multilevel encryption Method**		
	Image 1	Image 2	Image 3	Image 1	Image 2	Image 3	Image 1	Image 2	Image 3	Image 1	Image 2	Image 3
PSNR	7.9973	7.9945	7.999	9.3566	9.3530	8.3771	**7.7146**	**6.1370**	**5.4127**	**6.6420**	**5.3065**	**5.2011**
NPCR	99.56	99.59	99.61	99.58	99.60	99.71	**99.64**	**99.71**	**99.88**	**99.72**	**99.96**	**99.90**
UACI	33.50	33.49	33.48	33.31	33.37	33.32	**34.31**	**33.87**	**33.68**	**34.60**	**34.03**	**33.98**
CC	0.97	0.96	0.94	0.94	0.92	0.89	**0.98**	**0.97**	**0.99**	**0.99**	**0.98**	**0.99**

This evaluation report shows a comparison of modified vigenere cipher and multilevel encryption method with existing methods based on a few significant quality measure parameters like PSNR, NPCR, UACI, and CC. From this evaluation outcome, it is undoubtedly proved that the [8&9] methods provide superior results when compared to the existing methods.

CRYPTANALYSIS

Cryptanalysis is the study of breaking the cipher text without using original key. The main goal of cryptanalysis is gaining knowledge of the encrypted text without the key [1]. It is a major part of modern cryptology and focuses on the security analysis of different kinds of cryptography algorithms. In cryptanalysis attack, there are two possibilities either the cryptanalyst might have cipher text and want to discover the plaintext or the cryptanalyst might have cipher text and want to discover the encryption key that was used to encrypt the message [5].

The algorithm standard and quality of modified vigenere cipher [9] and multilevel encryption methodology [10] are evaluated by using three types of attacks described below,

Cipher text only attack

In this attack [4] the cryptanalyst knows only the encrypted text. So the attackers can identify the length of the cipher is performed to find the length of the key. To identify the period Index of Coincidence is a method to assess the strength of the proposed algorithm.

Index of coincidence (IC)

The Index of Coincidence (**IC**) is a cryptanalysis technique, studying the probability of finding repeating letters in a ciphered text.

$$\text{IC} = \frac{\sum_{i=A}^{i=z} fi(fi-1)}{N(N-1)}$$

fi is the count of the letter, *i* in the cipher text (where *i=A,B,………….Z*) and *N* is the total number of letters in the cipher text. When the IC value is high it signifies the strongest approach of the proposed algorithm. [1]

Known plaintext attack

The cryptanalyst knows the plaintext in this category of attack [4]. The main target of this attack is to determine the key from the text which means to find the specific key. To find the specific key Chi squared statistic is a process to ensure the superiority of the proposed algorithm.

Chi-squared Statistic

It is a measure of how similar two categorical probability distributions are.

$$\text{Chi-squared statistic} = \chi^2(C,E) = \sum_{i=A}^{i=z} \frac{(Ci - Ei)^2}{Ei}$$

Where C is the count of letter A and E is the expected count of letter A. When the two distributions are identical, the chi-squared statistic is 0, when the distributions are very different some higher number will be the result [1].

Brute force attack

It is an attack on an encrypted message that simply attempts to decrypt the message with every possible key [4]. An attacker could try a brute force attack on the key table, even though that could be more time-consuming. In this modified vigenere cipher and multilevel encryption methodologies, the k_n number of keys are generated randomly depend upon the size of the input. Consequently, very long keys have used these methods, so the exact key could not be determined by using brute force attack and it is very complicated to find the specific key.

Cryptanalysis of Modified Vigenere Cipher and Multilevel Encryption Method

Three various types of DICOM images, such as Knee MR, Head CT, and Ankle X-Ray of varying sizes are taken as input for evaluation. The results are as follows,

Table 2: Index of coincidence by using modified vigenere cipher and multilevel encryption methodologies

S.No	Tag/Patient data Name	Size (KB)	Index of Coincidence Value	
			Modified Vigenere cipher	Multilevel Encryption Methodology
1	Knee MR data	388	0.0634	0.0637
2	Head CT data	129	0.0632	0.0639
3	Ankle X-Ray	513	0.0648	0.0659

When the incidence of coincidence value high (close to 0.070), it represents then the message has been probably encrypted using a poly alphabetic cipher.

Table 3: Chi squared Statistic by using modified vigenere cipher and multilevel encryption methodologies

S.No	Tag/Patient data Name	Size (KB)	Chi squared statistic Value	
			Modified Vigenere cipher	Multilevel Encryption Methodology
1	Knee MR data	388	1362.0874	1474.4985

2	Head CT data	129	1316.9510	1408.0931
3	Ankle X-Ray	513	1374.8927	1417.5792

Chi-squared statistic is a measure of how similar two categorical probability distributions are. When the distributions are very different some higher number will be the result.

Cryptanalysis Performance Evaluation

For a normal English text of alphabet of A-Z, the Variance is usually 14.50603 and the standard deviation of 3.80868. The following analysis result shows that the proposed algorithms are said to be perfect secrecy,

Table 4: Performance Analysis

Cryptanalysis Evaluation Measures	**Existing methods**		**Proposed Methods**	
	A Crypto system based on vigenere cipher with varying key [6]	A Hybrid Crypto system Based on Vigenere Cipher And Columnar Transposition Cipher [7]	Modified Vigenere Cipher	Multilevel Encryption Method
Index of Coincidence	0.0631	0.0501	**0.0648**	**0.0659**
Chi-squared statistic against English distribution	1008.8847	655.8480	**1374.8927**	**1417.5792**
Chi-squared statistic against uniform distribution	62.1864	38.7778	**68.6183**	**71.2796**
Statistical data: variance	15.5918	33.9517	**34.6158**	**36.5060**
Statistical data: standard deviation	3.9487	5.8268	**5.9630**	**5.9886**

From the above table it clearly is shown that the high values of IC and chi-squared statistic due to its different distributions. The standard deviation results indicate there is a larger deviation compared with previous methods. From the results, it is evident that these methods provide better results when compared with the existing ones.

CONCLUSION

In this paper, the efficiency of the methods namely modified vigenere cipher and multilevel encryption method are studied. The performance of the modified vigenere cipher and multilevel encryption methodology is evaluated by various quality measures like PSNR, UACI, NPCR, and CC. The comparison between these two methods as well as with the existing methods [10&11] are tabulated. In cryptography, the algorithm quality and standard are acceptable only after the cryptanalysis validating. In this paper, the cryptanalysis is done using measures such as Index of coincidence, Chi-squared statistic against English distribution, Chi-squared statistic against uniform distribution, Statistical data: variance, and Statistical data: standard deviation. The results of cryptanalysis show the greater efficiency and reliability of these [8, 9] two methods when compared to existing methods namely, A Crypto system based on vigenere cipher with varying key and A Hybrid Crypto system based on Vigenere Cipher and Columnar Transposition Cipher methods.

REFERENCES

[1] Cryptanalysis measures, characterization/chi-squared-statistic/, last accessed on 11.10.2015.

[2] Digital Imaging and Communications in Medicine (DICOM) Part 15: Security Profiles, Published by "National Electrical Manufacturers Association" USA, in 2003.

[3] DICOM security chapter 11, ACR-NEMA (National Electrical Manufacturers Association files, pp. 247-261.

[4] Douglas R. Stinson, "CRYPTOGRAPHY Theory and Practice", Second Edition, Chapman & Hall/CRC, ISBN 978-1584882060.

[5] Neetu Settia, "Cryptanalysis of Modern Cryptographic Algorithms", International Journal of Computer Science and Technology, Vol. 1, Issue 2, ISSN: 0 9 7 6 - 8 4 9 1, December 2010, 166-169.

[6] Quist-Aphetsi Kester, "A cryptosystem based on Vigenere cipher with varying key", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 10, December 2012, 108-113.

[7] Quist-Aphetsi Kester, "A Hybrid Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher", International Journal of Advanced Technology & Engineering Research (IJATER), ISSN No: 2250-3536 Volume 3, Issue 1, Jan. 2013, 141-147.

[8] P.Subhasri and Dr. A. Padmapriya, " Enhancing the Security Of Dicom Content Using Modified Vigenere Cipher", International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.55, May 2015, 1951-1956.

[9] P.Subhasri and Dr. A. Padmapriya, "Multilevel Encryption for securing DICOM content with Noise Removal", Communicated on Romanian Journal of Information Science and Technology (ROMJIST), December 2015.

[10] Ye Ruisong and Junming Ma, "An image encryption scheme based on hybrid orbit of hyper chaotic systems", I. J. Computer Network and Information Security, 2015, 25-33.

[11] Zainal and Ali Abdulgader et al, "Enhancement of AES algorithm based on chaotic maps and shift operation for image encryption", Journal of Theoretical and Applied Information Technology, Vol.71 No.1, January 2015, 1-12.

[12] B.Selvarani, "An Ideal Approach for Medical Data Security Using Partial Homomorphic Encryption", The International Journal of Pharma and Bio sciences (IJPBS), Special issue SP02 "Healthcare Technology and management", October 2016, 15-20.