

A Play-Fair Cipher Based Authentication Medical Data Image Transaction Process

Submitted By

Md. Rabiul Sani

ID : 191-17-391

Department of Management Information System (MIS)

Daffodil International University, Dhaka

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Master of Science (MS) in Management Information System (MIS).

Supervised by

Md. Zahid Hasan

Assistant Professor

Department of Computer Science and Engineering (CSE)

Daffodil International University, Dhaka



Daffodil International University

Dhaka, Bangladesh

December, 2019

APPROVAL

This thesis titled “A Play-Fair Cipher Based Authentication Medical Data Image Transaction Process”, submitted by Md. Rabius Sani, ID No: 191-17-391 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of MS in Management Information System and approved as to its style and contents. The presentation has been held on 08th December 2019.

BOARD OF EXAMINERS



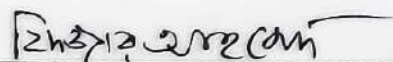
Dr. Syed Akhter Hossain
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman



Dr. Sheak Rashed Haider Noori
Associate Professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Fizar Ahmed
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



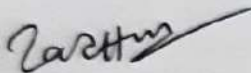
Dr. Mohammad Shorif Uddin
Professor
Department of Computer Science and Engineering
Jahangirnagar University

External Examiner

Certification

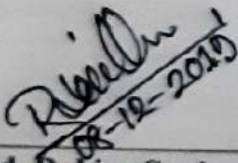
This is to certify that this thesis entitled “**A Play-Fair Cipher Based Authentication Medical Data Image Transaction Process**” is done by the following students under my direct supervision and this work has been carried out by them in the Department of Computer Science and Engineering under the Faculty of Faculty of Science and Information Technology of Daffodil International University in partial fulfillment of the requirements for the degree of Masters of Science in Management Information System. The presentation of the work was held on 8th December 2019.

Supervised By:



Md Zahid Hasan
Assistant Professor
Department of Computer Science and Engineering
Daffodil International University

Submitted By:



Md. Rabius Sani
ID: 191-17-391
Department of Management Information System
Daffodil International University

ACKNOWLEDGEMENT

Firstly I give thanks to almighty Allah from the bottom of my hearts.

I would like to express my sincere gratitude to my honorable supervisor, **Md Zahid Hasan Assistant Professor, Department of Computer Science and Engineering**, DIU who inspired me in every moment. I am thankful to her for his continuous encouragement, kind co-operation, and scholastic guidance all along the thesis. He has always been extremely generous with his time, knowledge and ideas and allowed me great freedom in this research.

I express my humble gratitude to all teachers of Department of Computer Science and Engineering for their support in numerous ways throughout this project work. I am also grateful to the authors whose valuable research papers and books I have considered as reference in this thesis paper.

Apart from that, I would like to thank my friends for sharing knowledge; information and helping me in making this thesis a success. Also thanks for lending me some tools and equipment.

Finally I would like to thank my parents who have given us tremendous inspirations and supports. Without their mental and financial supports, I would not able to complete my thesis.

Md. Rabius Sani

ID: 191-17-391

Management Information Systems (MIS)

Daffodil International University

ABSTRACT

The medical images which contain patient information need to be transaction from one doctor to another doctor. Patients who live in a remote area are able to communicate with the healthcare provider and benefit from the doctor consultations. However, it has been a challenge to provide a secure telemedicine system, which captures user's mobility and patient privacy. Message authentication is a mechanism or service, used to verify the integrity of a message. Integrity and source authentication is achieved by using Message Authentication Codes. The Play-fair cipher is a manual symmetric encryption cipher. The play-fair cipher starts with creating a key table. The key table is a 5×5 grid of letter. This application apply to Network security, personal data protection, payment security, database secure, preservation and confidentiality of information.

Table of Contents

<u>Index</u>	<u>Page No</u>
APPROVAL.....	i
CERTIFICATION.....	ii
ACKNOWLEDGEMENT.....	iii
ABSTRACT.....	iv
LIST OF FIGURES.....	vii
LIST OF TABLE.....	xiii
LIST OF ABBREVIATIONS.....	ix
Chapter 1: Introduction	01 - 02
1.1 Introduction	01
1.2 Motivation	01
1.3 Objective	01
1.4 Report Layout	01
1.5 Summary	02
Chapter 2: Literature Reviews	03 - 07
2.1 Introduction	03
2.2 Related Works	03
2.3 Problem	07
2.4 Comparative Studies	07
2.5 Encryption And Decryption	07
2.5.1 Symmetric-Key Encryption	08
2.5.2 Public-Key Encryption	08
2.5.3 Key Length and Encryption Strength	09
2.6 Play-Fair Cipher	10
2.7 The Algorithm of Play-Fair Cipher	11
2.8 Discussion	12

Chapter 3: Proposed Model	13 - 29
3.1 Proposed Scheme	13
3.2 Concept	13
3.3 The Proposed Method	14
3.4 Pre-Processing Step	15
3.5 Algorithm 1: The Play-Fair Image Encryption	16
3.6 Algorithm 1: The Play-Fair Image Decryption	16
Chapter 4: Results And Discussion	18 - 37
4.1 Implementation	18
4.2 Key Space Analysis	18
4.3 Key Sensitivity Test	18
4.4 Visual Diffusion Test	18
Chapter 5: Conclusion	20 - 42
5.1 Conclusion	20
5.2 Future Scope	20
References	21

List of Figures

Chapter 2: Literature Reviews

2.1	Encryption using vigenere cipher and play-fair cipher	05
2.2	Decryption using Vigenere cipher and Play-fair cipher	05
2.3	The Encryption and Decryption Processes of a Cipher	06
2.5.1	Symmetric-Key Encryption	08
2.5.2	Public-Key Encryption	08

Chapter 3: Proposed Model

3.1	Process of the Encrypting Algorithm	13
3.2	Process of the Decrypting Algorithm	13
3.3	Process of the Encryption & Decrypting Algorithm	14
3.4	Encryption & Decryption Engine	15
3.5	Show Steps of Encryption and Decryption Operations	17

List of Table

Chapter 2: Literature Reviews

2.1 A Classical Play-Fair Matrix 04

2.2 The Algorithm of Play-fair Cipher 09

Chapter 4: Results And Discussion

4.1 PSNR Values for Standard Images and Various Cipher Images Using Different Secret Keys 13

List of Abbreviations

- MIC : Medical image computing
PSNR : Peak Signal-To-Noise Ratio
MSE Mean Square Error

Chapter - 1

INTRODUCTION

1.1 Introduction

Restorative picture handling (MIC) is an interdisciplinary research at the crossing point motivation behind programming structuring, data building, electrical arranging, material science, number shuffling and arrangement. Helpful imaging improvement acknowledge an imperative movement in the present human organizations framework. Right now the medicinal pictures which contain tireless data should be exchange starting with one master then onto the accompanying expert at colossal. Where, Patients who live in a remote district can converse with the human organizations supplier and bit of slack from the professional discoursed. Confirmation is a fragment or association of checking the character of an individual or gadget. The endorsement association is worried over guaranteeing or surveying that a correspondence or transection is Authentic. It is a touch of typical step by step nearness in the mechanized age. While it helps keep our own data private, it isn't confirm. It will a test to be given a guaranteed telemedicine framework, which gets clients (patients and specialists) adaptability and patient security.

1.2 Motivation

The dangerous improvement in PC structures and their interconnection by techniques for structure has expanded the reliance of the two affiliations and people on the data set away and passed on utilizing these frameworks which partner has prompted a motivated awareness of the need to shield information and assets from gatecrashers. (Jitendra et al., 2013). Cryptography is the structure of unequivocal systems for guaranteeing the riddle similarly as realness of data. The need of cryptographic check is to keep up a key decent ways from peril to tolerability, request and accessibility. In each zone, assortment of data or move of information with a vital level of security is required. Thusly a solid encryption strategy is required. This evaluation centers around play reasonable figure check which is particularly solid what's more requires less memory and power. Be that as it may, a colossal exertion has been done in breaking down Play reasonable figures of different sizes, this perception rouses the appraisal did in this proposition.

1.3 Objective

This chapter has several objective:

- ✚ To define three security goals.
- ✚ To introduce two techniques, cryptography and play fair cipher, to implement security mechanisms.
- ✚ To define security service mechanisms to provide security service.
- ✚ To define security service and how they are related to the three security goals.

I am alive in the data stage. I have to possess data near each bit of my lives. Continuously end, data is a bit of leeway that has a worth like some other resource. As a favorable position, Information should be checked from assaults. To be affirmed, data should be kept up a vital good

ways from unapproved get to (Confidentiality), Protected from unapproved change (Integrity), and open to a confirmed segment when it is required (Availability).

1.4 Report Layout

The layout of this report is described below:

1. In chapter 1 I have covered the introduction to my project, motivation for building this kind of system, objectives and goals of the A Play-Fair Cipher Based Authentication Medical Data Image Transaction Process, what I have planned or the expected outcome of the application and the ultimate layout of this report.
2. In chapter 2 I have added some related projects and some case studies that helped me a lot in developing this application. I also included the problems and challenges that I faced during the research development phase.
3. In chapter 3 I have specified the whole process of this application using some use case diagrams, state diagrams, business process models and work flow diagrams.
4. In chapter 4 I included the specification that I have used in the system. Front-end design, back-end design, UI/UX, implementation etc. requirements are described in this chapter too.
5. In chapter 5 I have added the implementation and testing details and analysis reports in details.
6. Chapter 6 is covered by the discussion and future development scopes and plans.

1.5 Summary

Firstly I discuss about Medical Image Data, Data Transection. Then I discuss about Motivation, Objective, methodology and finally discuss about report layout of my thesis.

CHAPTER - 2 LITERATURE REVIEW

2.1 Introduction

In this section, I self-control discussion about the related works, case studies, scope of the problem, challenges. After fixing the plan I have started studying on some other related applications and case studies. Summarize of those are added in this chapter.

2.2 Related Works

I have checked and tried to understand some A Play-Fair Cipher Based Authentication Medical Data Image Transaction Process. Some of them are listed below.

1. A Survey on Play-fair Cipher Encryption Technique.
2. A Line for Attractive the Safety of Play-fair Cipher.
3. A Modified Play-fair Cipher for Encrypting Digital Images.

The renowned multi letter cipher encryption system is play-fair cipher despite the fact that, an extensive variety of techniques have been employed for encryption and decryption the play-fair cipher shows a great development over other encryption method. It consists of 5x5 key matrix. Play-reasonable is the sort of square figure which was no detainment to the proportion of fonts in a message it can do, yet it handles square of characters scrambling, unraveling two letterings in a suffering development.

Cryptography is a field of information security which is appeared to offer security to the senders and beneficiaries to transmit and get delicate information through a risky channel by a systems for process called Encryption and Unscrambling. Cryptography guarantees that the message ought to be sent with no changes and essentially the certified individual can have the decision to open and look at the message. Diverse cryptographic frameworks and figurings are made for accomplishing secure correspondence.

In this paper, analyzed about the old style play sensible figuring, its advantages awful checks and other related work done in this field. The customary play sensible figuring relies upon the usage of a system to literatures built by means of a watchword. This figure count can simply allow the substance that contains simply letter sets. The present play sensible figure estimation relies upon with usage of 5 X 5 structure to letters created using a watchword. In this a watchword 'Government' was used to the cross section was worked by satisfying. The literatures of catchphrase from left site to right site to absolutely filling in the rest of grid with the remaining alphabetic solicitation

Cryptography Equation

Equation for encryption

$$C = [EKs (Plaintext)] \dots\dots\dots 1$$

Equation for decryption

$$P = [DKs (Cipher text)] \dots\dots\dots 2$$

Table 2.1: A Classical Play-fair Matrix

W	O	R	D	A
B	C	E	F	G
H	I/J	K	L	M
N	P	Q	S	T
U	V	W	Y	Z

The utilization of web is rising rapidly. So there are more necessities to check the information transmitted over different structures utilizing arranged security associations. To give the security to the system and information different encryption procedures are utilized. [1]

This paper presents an investigation on play-sensible figure. It is a multi-letter figure system. Recently redesigned the play-sensible figure using 6x6 matrix, 8x8 system and 16x16 structure. These system encodes just letters all together just as numerals and extraordinary character. It furthermore shows spaces among words and some encryption structures uses particular square for different letters all together, numerals and remarkable character. The comprehensive and changed play-sensible structure play has diverse ideal conditions over fundamental play-sensible figure count is proper for real application.

Another system present secure transmission of message by changed variety of Play reasonable figure with Discretionary number generator procedures getting together with Vigenere figure. To build up this approach for encryption methodology, no doubt the least requesting strategy for erratic number generator procedures called straight congruential generator has been utilized. Play reasonable figure approach subject to polyalphabetic figure. It is ordinarily simple to break since regardless of all that it leaves a basic bit of the structure and two or three a couple of letters of figure content are adequate. In this we utilized twofold encryption and unscrambling technique. For the encryption, first encode the plaintext by vigenere figure, and from that point result scramble by play reasonable figure. Moreover, result is called figure content. After that we are mapping optional numbers to figure message and relating numbers will be transmitted to the beneficiary instead of in back to back solicitation letter. This framework quickly collects security of the transmission over an unbound channel.

There are different checks that are utilized so far for encryption of various file setup like substance record, sound record, pictures and narratives. While different calculations are open for encryption. A touch of the calculations that are utilized for encryption are RSA technique (Rivest, Shamir, Aldeman), DES (Data Encryption Standard), Play reasonable figure to Vignere figure. The estimation utilized in this work area work for encryption and unscrambling of substance record is Play reasonable figure and vigenere figure which is consistently ground-breaking to the degree time and security.

Steps for Encryption

1. The letters all calm and numbers are set in 6x6 Play sensible key system subject to watchword.
2. Produce 6x6 unique open number lattice using the direct congruential generator strategies.

3. Guide the Play sensible key cross section with the self-assertive number network.
4. Encode the plain substance P using Vigenere figure with key k1 and get quick result X
5. By then this result encode via Play practical figure with tag K2 and get figure content C
6. Find the distinct number with figure content C, the ready plan of these sum is convey to heir.

Steps for Decryption

1. Beneficiary get the movement of numbers.
2. Discover the figure content C relating to social event of number.
3. Read the figure content C utilizing the Play sound figure with tag K2 and get interim effect X.
4. Likewise, from that point X is decoded by vigenere figure with key k1 and get plaintext P.

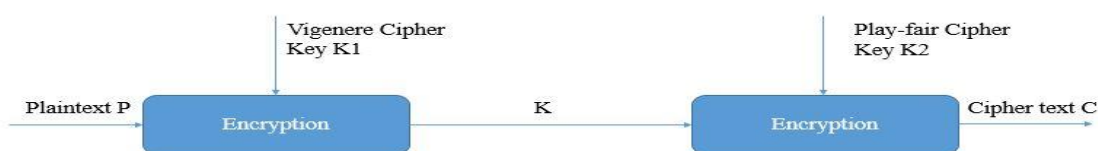


Figure 2.1: Encryption using vigenere and cipher and play-fair cipher

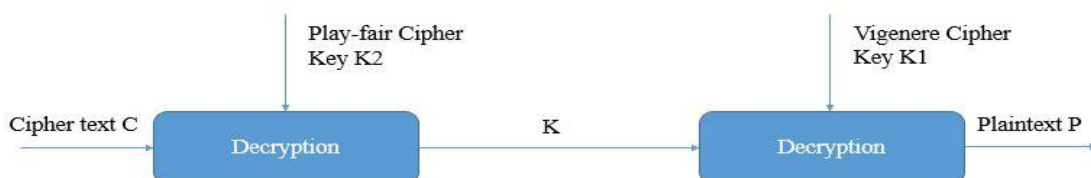


Figure 2.2: Decryption using Vigenere cipher besides Play-fair cipher

To finish balanced Play-reasonable figure utilizing abstract number age. We utilize direct congruential generator strategy that can be utilized to make phenomenal arranged self-emphatic groupings by changing increment and multiplier. [2].

The customary Play-reasonable figure isn't check considering the way that it makes just 676 structures. We use vigenere figure and Play-reasonable figure for encryption and unwinding. We are mapping erratic number approach to figure message and relating number will be transmitted to the beneficiary rather than in back to back solicitation letter. This technique broadens security of the transmission over unbound channel. Since we utilize 6x6 system that produces 1296 structures and in addition use vigenere figure that produces 456976. The complete structures

produces will be $1296 \times 456966 = 592240896$. The future work will consider, to makes the size of framework to join the outstanding character.

In this paper, another augmentation of the Play-reasonable figure calculation is proposed to scramble picture information much more safely. The proposed framework develops a 16×16 riddle key structure to scramble picture information byte by byte. Likewise, the check multifaceted nature is broadened utilizing veiling to XOR agenda. at is, the key was utilized convey a shroud that was then XORed to the mixed picture. Exploratory outcomes demonstrated that utilizing two inconsequential fascinating riddle keys, the resultant blended pictures are still totally remarkable. As the general people wound up being consistently mindful of cryptographic uses, the individual and social need for security is broadened. These days, cryptography proposed only to encryption, which was way to altering standard data (decoded message) with puzzled drivel (i.e., encoded message). Unscrambling is the adjust, as appeared in figure 1, moving from the questionable blended message back to decoded message. A figure is a few estimations that make the encryption and the rotating unscrambling.

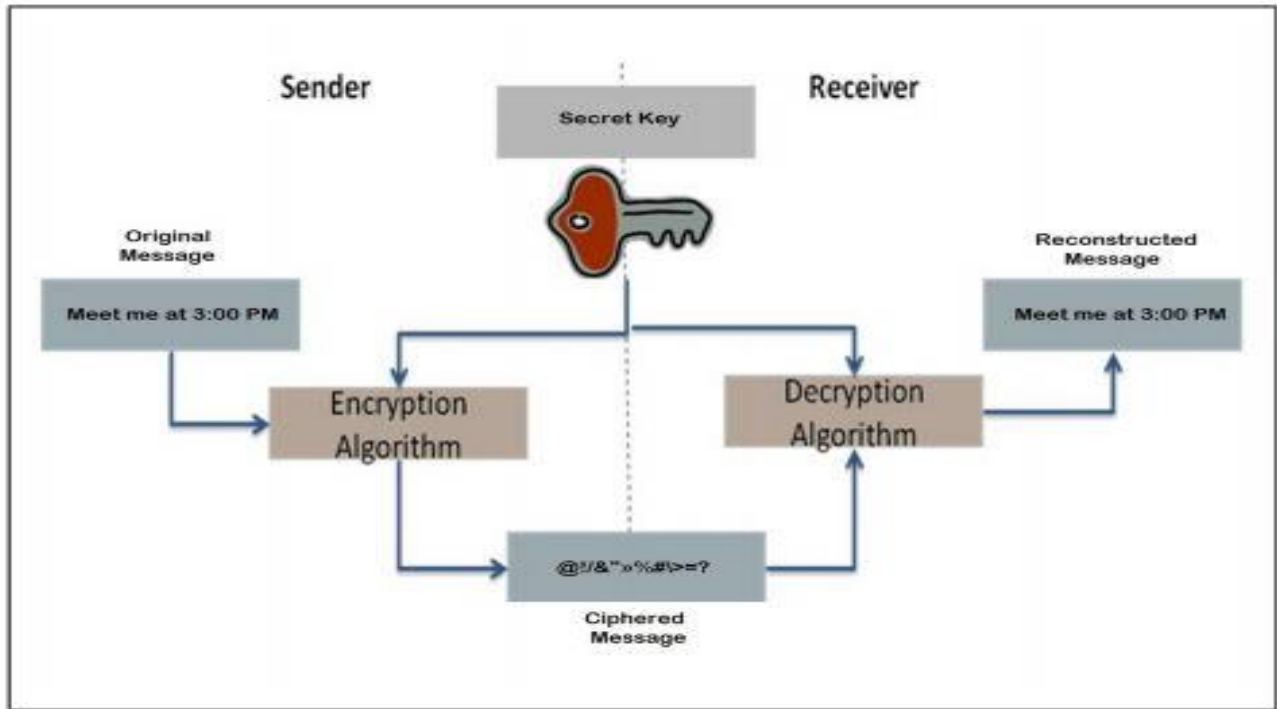


Figure 2.3: The Encryption message and Decryption message Processes of a Cipher text

The classic Play-fair Cipher can only be useful for a plain-text consisting of alphabets. However, a number of recently proposed extensions succeeded to encrypt alphanumeric data using different approaches. In this paper, we present another extension for encrypting image content. So, instead of the classical 5×5 matrix, the proposed method constructs 16×16 key matrix for a better alignment with image pixel data. In addition, an XOR procedure has been adopted for a more secure and yet scrambled results.

2.3 Problem

As I noted above, classical Play fair cipher has some weak points. Among those vulnerabilities is that much of the language structure such as numbers and punctuation are not represented. So, recent research focused on finding ways to enhance the Play fair cipher and avoid some of its disadvantages.

For example, Ravindra et al. proposed an extension to the traditional Play fair algorithm. Their approach suggested using a 6×6 matrix instead of 5×5 . The matrix is constructed in a similar way with the classic technique except that beside the set of alphabets this matrix is large enough to accommodate numerical digits (0 to 9) as well. Furthermore, the I/J was not counted as one letter. Instead, Ravindra et al. placed I and J in two separate cells in order to avoid ambiguity at decryption time.

Another solution was proposed in the light of the new emerging field of bioinformatics. That is, Sabry et al. proposed a DNA in addition to Amino Acids-Based Play fair Cipher-text algorithm that enables the user to use any combination of alphabets, numbers, special characters, or even spaces a plain-text. The encryption method starts by addressing the data in twofold structure, which is later changed into groupings of DNA nucleotides. Thusly, these nucleotides experience a Play fair encryption process subject to amino-acids structure. Those various forms can match different applications such as in.

Currently, a new extension of classical Play fair cipher was presented by Hamad et al. in. The proposed ciphering technique provides 8×8 amino acid codons substitution matrix. Furthermore, an interweaving step was added for more secured results.

2.4 Comparative Studies

After reviewing some other similar approaches and their case studies I have sorted common features and unique features of each. Most of them are built for specific purpose for their own demand.

2.5 Encryption Message and Decryption Message

Encryption was the course to changing data so that was uncertain to anybody yet the orchestrated beneficiary. Interpreting is the course toward changing blended data in with the target that it is justifiable once more. A cryptographic calculation, besides called a figure, is a numerical point of confinement utilized for encryption or interpreting. An extraordinary piece of the time, two related points of confinement were utilized, one encryption besides other on behalf of unscrambling.

With most outrageous current cryptography, capacity to keep blended substances confound was amassed not concerning the cryptographic figuring, which was ordinarily known, yet on a number called a key that must be utilized with the tally to make an encoded outcome or to unscramble starting late encoded data. Unscrambling with the right key is central. Unscrambling without the right key is ungainly, and now and again gigantic for every single reasonable clarification. The zones that quest for after present the utilization of keys for encryption and unscrambling.

 Symmetric-Key Encryption Message.

- ✚ Public-Key Encryption Message.
- ✚ Key Length to Encryption Strength Message.

2.5.1 Symmetric-Key Encryption

Through symmetric-key encryption message, the encryption key can be resolved from the disentangling key and a changed way. With most symmetric counts, a comparable key is used for both encryption and sorting out, as shown in Figure 2.4.

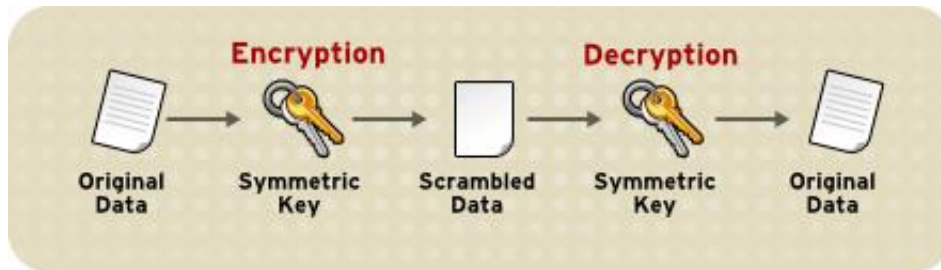


Figure 2.4: Symmetric-Key Encryption

Executions of symmetric-key encryption can be profoundly proficient, with the goal that clients don't encounter any critical time delay because to the encryption besides decoding. Symmetric-key encryption message likewise gives an equal to verification, data scrambled by unique symmetric key can't be unscrambled with some other symmetric key. Accordingly, as long as the symmetric key was stayed quiet to the double gatherings utilizing it to encode interchanges, each gathering can be certain that it is speaking by the different providing the decoded mails keep on appearing well and good.

Symmetric-key encryption message was convincing just if the symmetric key was remained mindful through the two parties included. If some other individual finds the key, it impacts both strategy and underwriting. A person with an unapproved symmetric key not solely can unscramble messages sent with that key, yet can scramble new messages and send them as if they started from one of the two parties who were from the beginning using the key.

Symmetric-key encryption recognize a huge development in the SSL show up, which is completely used for certification, change insistence, and encryption over TCP/IP structures. SSL besides uses procedures for open key encryption, which is delineated in the going with zone.

2.5.2 Public-Key Encryption

The most usually utilized usage of open key encryption depend on controls licensed by RSA Data Security. Accordingly, this part portrays the RSA way to deal with open key encryption.

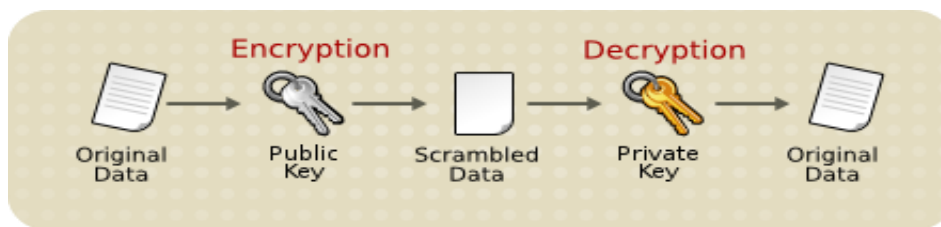


Figure 2.4: Public-Key Encryption

Open key encryption (additionally called hilter kilter encryption) includes a couple of keys—an open key and a private key-related with an element that necessities to verify its personality electronically or to sign or encode information. Every open key is distributed, and the relating private key is stayed discreet. Information scrambled with your open key can be decoded uniquely with your private key. Figure 2.4 shows a disentangled perspective on the manner in which open key encryption works.

The plan appeared in Figure 2.4 lets you openly convey an open key, and just you will have the option to peruse information encoded utilizing this key. By and large, to send scrambled information to somebody, you encode the information with that individual's open key, and the individual accepting the encoded information decodes it with the comparing private key.

Contrasted and symmetric-key encryption, open key encryption requires more calculation and is along these lines not constantly proper for a lot of information. Be that as it may, it's conceivable to utilize open key encryption to send a symmetric key, which would then be able to be utilized to encode extra information. This is the methodology utilized by the SSL convention.

As it occurs, the switch of the plan appeared in Figure 2 additionally works: information scrambled with your private key can be decoded distinctly with your open key. This would not be an alluring method to encode delicate information, be that as it may, in light of the fact that it implies that anybody with your open key, which is by definition distributed, could decode the information. By and by, private-key encryption is valuable, since it implies you can utilize your private key to sign information with your computerized mark a significant prerequisite for electronic trade and other business uses of cryptography. Customer programming, for example, Firefox would then be able to utilize your open key to affirm that the message was marked with your private key and that it hasn't been altered since being agreed upon. "Computerized Signatures" portrays how this affirmation procedure works.

2.5.3 Key Length and Encryption Strength

Breaking an encryption calculation is fundamentally finding the way in to the entrance the encoded information in plain content. For symmetric calculations, breaking the calculation ordinarily implies attempting to decide the key used to encode the content. For an open key calculation, breaking the calculation for the most part implies procuring the common mystery data between two beneficiaries.

One strategy for breaking a symmetric calculation is to just attempt each key inside the full calculation until the correct key is found. For open key calculations, since half of the key pair is freely known, the other half (private key) can be determined utilizing distributed, however intricate, numerical computations. Physically finding the way to break a calculation is known as an animal power assault.

Breaking a calculation presents the danger of capturing, or in any event, mimicking and falsely checking, private data. The key quality of a calculation is controlled by finding the quickest strategy to break the calculation and contrasting it with an animal power assault.

For symmetric keys, encryption quality is regularly depicted as far as the size or length of the keys used to play out the encryption: all in all, more extended keys give more grounded encryption. Key length is estimated in bits. For instance, 128-piece keys for use with the RC4 symmetric-key figure bolstered by SSL give fundamentally preferred cryptographic insurance over 40-piece keys for use with a similar figure. Generally, 128-piece RC4 encryption is 3 x multiple times more grounded than 40-piece RC4 encryption. (For more data about RC4 and different figures utilized with SSL, see "Prologue to SSL.") An encryption key is viewed as full quality if the most popular assault to break the key is no quicker than a beast power endeavor to test each key plausibility.

2.6 Play-fair Cipher

The Play fair Cipher is a manual symmetric encryption cipher invented in 1854 by Charles Wheatstone, however its name and popularity came from the endorsement of Lord Play fair.

The Play reasonable figure scrambles sets of letters (digraphs), rather than single letters just like the case with less difficult substitution figures, for example, the Caesar Figure. Recurrence examination is as yet conceivable on the Play reasonable figure, anyway it would be against 600 potential sets of letters rather than 26 various potential letters. Thus the Play reasonable figure is considerably more secure than more seasoned substitution figures, and its utilization proceeded up until WWII.

The play reasonable figure begins with making a key table. The key table is a 5×5 matrix of letters that will go about as the key for scrambling your plaintext. Every one of the 25 letters must be exceptional and one letter of the letter set (generally Q) is discarded from the table (as there are 25 spots and 26 letters in the letters in order).

Now for the actual encryption process. The Play fair cipher uses a few simple rules relating to where the letters of each digraph are in relation to each other. The rules are:

- ✚ On the off chance that the two letters are in a similar section, take the letter underneath every one (returning to the top if at the base)
- ✚ On the off chance that the two letters are in a similar line, take the letter to one side of every one (returning to one side if at the most remote right)
- ✚ In the event that neither of the previous two standards are valid, structure a square shape with the two letters and take the letters on the flat inverse corner of the square shape

The Play reasonable figure was utilized for the most part to secure significant, yet non-basic privileged insights, as it rushes to utilize and requires no extraordinary gear. When foe

cryptanalysts could break the code the data it was securing would regularly never again be important.

2.7 The Algorithm of Play-fair Cipher

The key used for a play fair cipher was usually to word, for the sake of example I motivation choose 'monarchy'. This is then used to generate a 'key square', e.g.

Table 2.2: The Algorithm of Play-fair Cipher

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Any grouping of 25 letters can be utilized as a key, insofar as all letters are in it and there are no reshapes. Note that there is no 'j', it is joined with 'I'. We currently apply the encryption rules to encode the plaintext.

- ✚ Expel any accentuation or characters that are absent in the key square (this may mean illuminating numbers, accentuation and so on.).
- ✚ Distinguish any twofold to letters in plaintext by supplant the next occurrence by a 'x' for example 'Tammer' - > 'Tamxer'.
- ✚ On basis off casual that the plaintext has an odd number of characters, add a 'x' as far as possible to make it even.
- ✚ Disruption plaintext hooked on sets of cultures, for example 'Tamxer' - > 'Ta mx er'
- ✚ To calculation currently chips away at every one to the letter sets. Locate to letters on the key square,

1.

```
a * * m *
* * * * *
* * * * *
s * * l *
* * * * *
```

Therefore, la => sm

2.

```
* * * * *
* b d h y
* * * * *
* * * * *
* * * * *
```

Hence, bh => dy

3.

```
** q **
```

```
** w **
```

```
*****
```

```
** n **
```

```
** y **
```

Hence, $qn \Rightarrow wy$

2.8 Discussion

The Play reasonable Figure was a quick better approach to encipher messages. It was the first of its sort, and opened up the universe of cryptography to a totally different kind of figure: the polygraphic figure. In spite of the fact that not verify as far as present day cryptography, it was a generous improvement over Monoalphabetic Substitution Figures, and essentially simpler to use in the field than Polyalphabetic Substitution Figures.

Chapter - 3 PROPOSED MODEL

3.1 Proposed Scheme

The basic concept of the proposed scheme is described in Section 3.2. The encrypted secret image is presented in Section 3.3. The steganography method is discussed in Section 3.4. Finally, integrity check using the SHA-512 hash function is presented in Section 3.5.

3.2 Concept

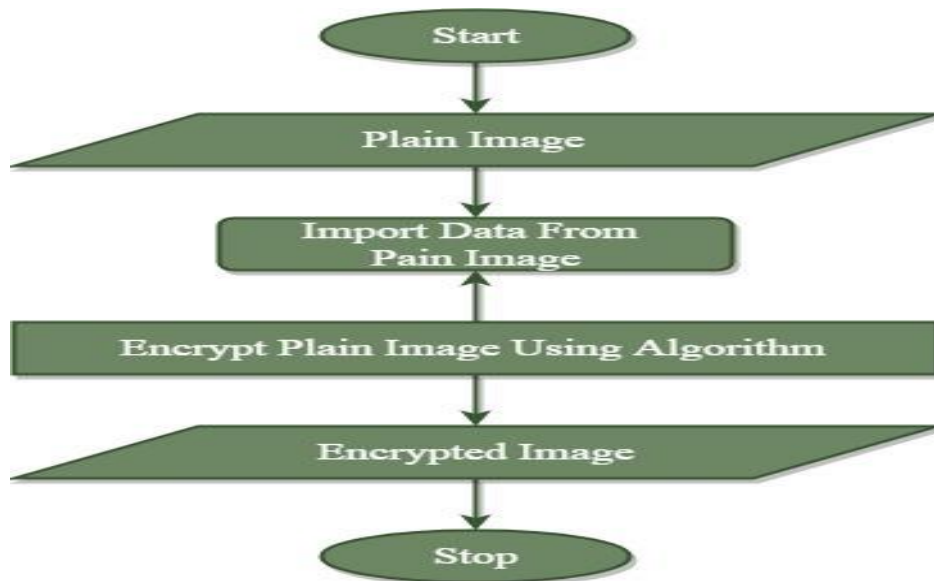


Figure 3.1: Process of the Encrypting Algorithm



Figure 3.2: Process of the Decrypting Algorithm

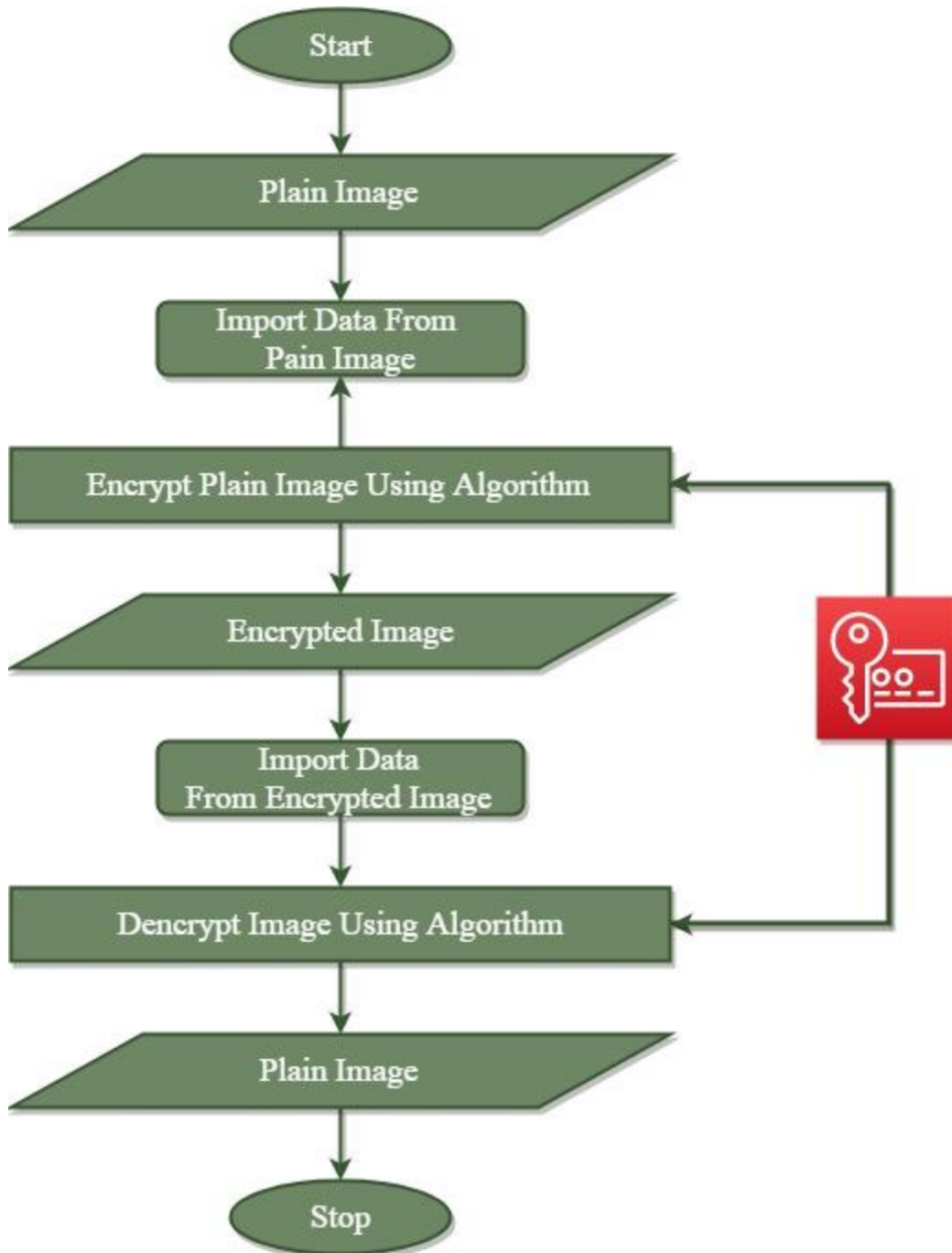


Figure 3.3: Process of the Encryption & Decryption Algorithm

3.3 The Proposed Method

In this paper, I introduce an improvement over the Play-fair cipher in order to apply it on image data. It is known that a pixel in a true colored image has three shading parts: RED, GREEN, and BLUE. Their values range is between 0 and 255. So, using a matrix of size 16×16 filled with values between 0 and 255 can be a perfect solution to encrypt color values directly into other intensity levels. Here, the key is expected to be an integer number that is supplied as the seed an incentive

in an arbitrary stage module to arbitrarily develop the substitution lattice. Then, the Play fair encryption process can be applied on pairs of the pixels color components in the plain image. The resultant scrambled image is not the final output yet. However, the proposed system adopts an XOR operation as an additional step to improve security. Here, the secret key is used once more to generate a random mask that has the same dimensions as any of the image's color component matrices. This random mask is XORed with the scrambled image in order to produce the cipher-image. This additional step process guarantees that the resultant cipher picture is totally unique in relation to the plain picture regardless of whether two comparative keys were utilized. Figure 3.3 gives an overview of the proposed ciphering system or a more detailed look, Algorithms 1 and 2 list the steps of the encryption and the decryption processes respectively.

3.4 Pre-Processing Step

For all the pixels in the image, do the following steps,

It was moreover titled as open key cryptography. It uses two keys: open key, which was known to people overall, utilized for encryption and private key, which is known obviously to the client of that key, utilized for unraveling. People generally speaking and the private keys are identified with one another by any numerical procedures. So to speak, information encoded by one open key can be blended uncommonly by its relating private key. Encryption and translating system as appeared underneath in figure 3.4:

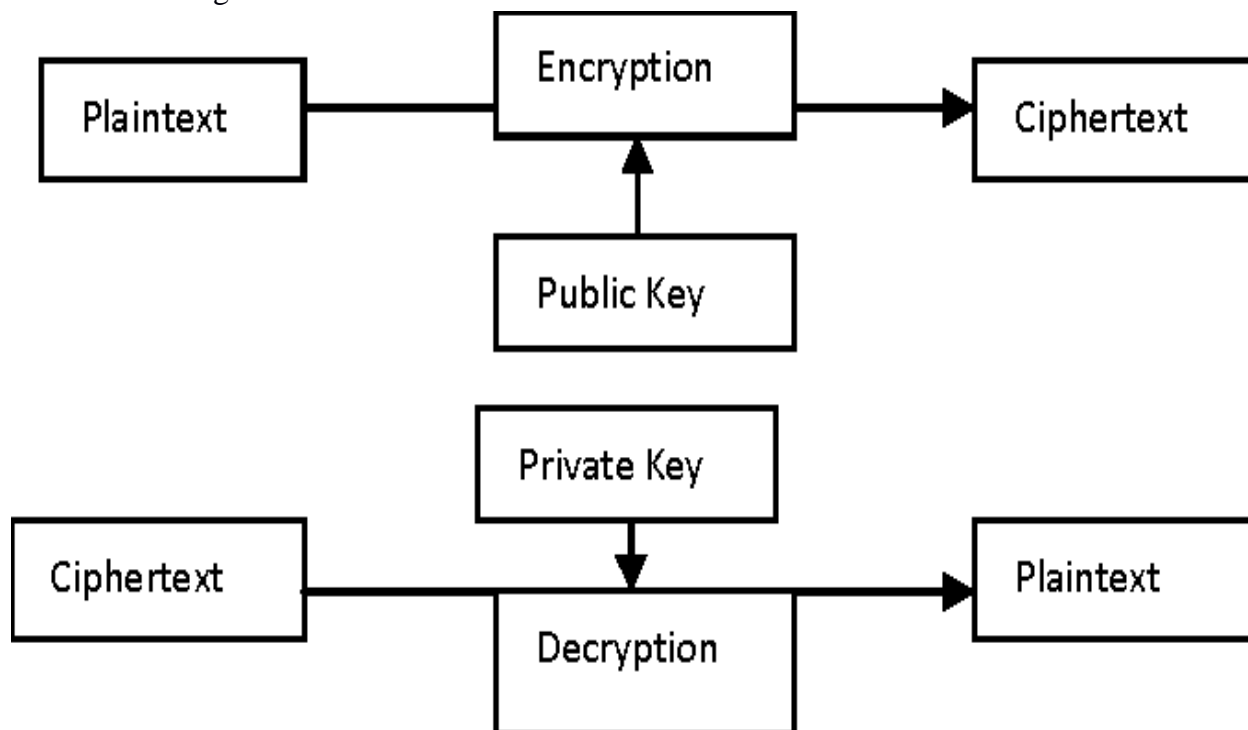


Figure 3.4: Encryption & Decryption Engine

3.5 Algorithm 1: The Play-Fair Image Encryption

Encryption algorithm: Image Encryption

Input: Plain image and Secret key

Output: Cipher image

- ✚ Read the plain image as RED, GREEN and BLUE matrices.
- ✚ If the plain image has an odd-number dimension append a row or column of zeros to the end to make it even.
- ✚ Construct a Key Square: 16 x16 matrix of random integer numbers between 0 and 255 using the secret key.
- ✚ For each pair of colors components in the RED plane of the plain- image do the following:
 - ✚ XOR the resultant scrambled image with the generated random mask.
 - ✚ Repeat step 4 to 6 for GREEN and BLUE color planes of the plain image.
- ✚ Return the resultant image as the cipher image.

3.6 Algorithm 2: The Play-Fair Image Decryption

Decryption Algorithm: Image Decryption

Input: Cipher image and Secret key.

Output: Plain image.

- ✚ Read the Cipher image as RED, GREEN and BLUE matrices.
- ✚ Use the secret Key to generate a mask made up with a random permutation of the numbers between 0 and 255.
- ✚ XOR the RED color plane of the Cipher image with the generated random mask.
- ✚ Construct a Key Square: 16×16 matrix of random integer numbers between 0 and 255 using the secret key.
- ✚ For each pair of the resultant XORed RED plane of the Cipher image do the following:
 - ✓ If the qualities are in various lines and segments, supplant the pair with the qualities at the contrary corners of the square shape characterized by the first match and keep up their request.
 - ✓ If the qualities point up on a parallel line of the lattice, oust them by the qualities to their prompt exact distinctly (folding over too one side).
 - ✓ If the qualities highlight to the similar section of the grid, (folding over to the top side of the segment).Repeat step 3 to 5 for GREEN and BLUE color planes of the cipher image.
- ✚ Return the resultant image as the Plain-image.

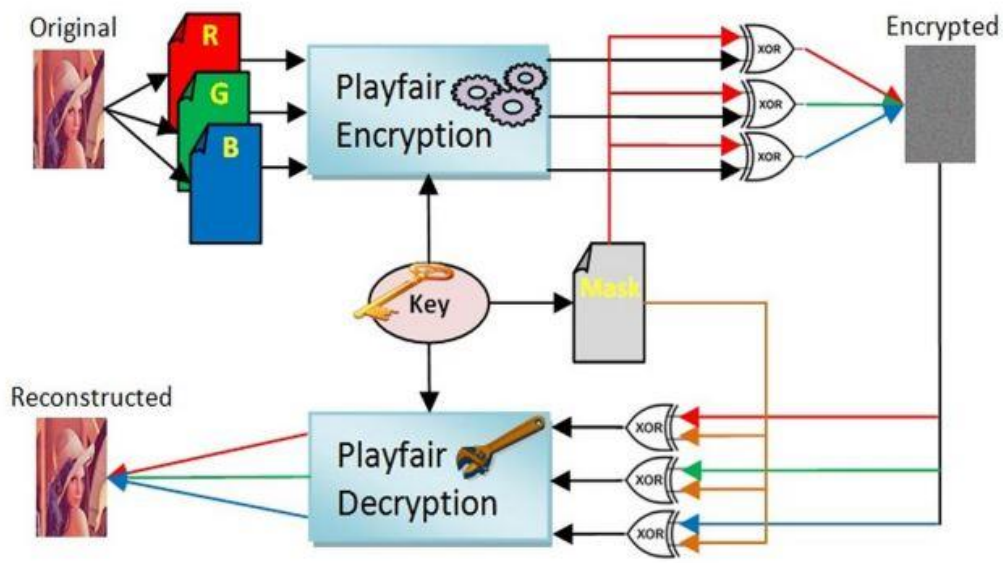


Figure 3.5: Show Steps of Encryption and Decryption Operations

Chapter - 4

Results and Discussions

4.1 Implementation

The proposed Play fair method was implemented using MATLAB version: 8.0.0.783 (R2012b). Three standard RGB color images were used for benchmark comparisons in size of 512*512. Figure 3.5 displays result to proposed encryption method consuming "21987" as secret key on the three test images. Obviously the results show the randomness of the resultant ciphered images.

4.2 Key Space Analysis

Cryptanalysis is a field that endeavor to find strategies to decode a message without earlier information on it figuring technique. Cryptanalysis is the thing that the layman calls "breaking the code". Together with cryptography they are called cryptology. In conventional Play reasonable figure, getting the key is moderately direct if both plain-content and figure content are known. Be that as it may, generally just the figure content will be accessible. In this manner, speculating a portion of the words dependent on information about the starting point of the message can be of an extraordinary assistance in remaking the substitution framework. It ought to be perceived that speculating a portion of the plain-content and utilizing that to reproduce the key square is by a wide margin the most effortless approach to split this figure. Cryptanalysis of the Play reasonable figure for picture is substantially more difficult than typical straightforward Play reasonable substitution figure, on the grounds that for this situation digraphs speak to sets of pixels rather than sets of letters. Applying a similar relationship of recurrence investigation requires examining 65536 pixel digraphs contrasted and just 676 if there should arise an occurrence of letter digraphs

4.3 Key Sensitivity Test

A few key affectability tests were performed utilizing various close key qualities. Figure 4 (b-f) shows the resultant figure pictures utilizing the key qualities: 21985, 21986, 21987, 21988 and 21989 separately. Figure 5 (b-f) shows the relating remade pictures utilizing increasingly shut faked key worthwhile the correct key is 21987. The outcomes demonstrate that the proposed strategy is touchy to the key. That is, a little difference in the key worth will bring about a totally different picture.

4.4 Visual Diffusion Test

More experimentation has been conducted to visually judge the diffusion in the resulted images using similar key values. The popular PSNR metric was employed as a similarity measure. PSNR be able to be computed by the ensuing method:

$$\text{PSNR} = 10 * \log\left(\frac{(\max f(x, y))^2}{\text{MSE}}\right)$$
$$\text{MSE} = \frac{1}{x * y} \sum_{x,y} (f(x, y) - p(x, y))^2$$

Where $f(x, y)$, $p(x, y)$ are the compared images of size $X*Y$ and MSE signifies the Mean Square Error. PSNR values are often expressed in decibels (dB) where the values will run to infinity if the two examined images are identical. Table 1 compares the PSNR values showing further information on the diffusion aspect using different keys on various standard images. In addition, a comparison of plain spitting image and cipher spitting image histograms is exposed in figure 4.1.

Table 4.1: PSNR Values for Standard Images and Various Cipher Images Using Different Secret Keys

		ORG	KEY = 21985	KEY = 21986	KEY = 21987
LENA	ORG	Inf	8.62	8.62	8.61
	KEY = 21985	8.62	Inf	7.75	7.74
	KEY = 21986	8.62	7.75	Inf	7.75
	KEY = 21987	8.61	7.74	7.75	Inf

Chapter - 5

Conclusion

5.1 Conclusion

The classic Play fair Cipher can only be useful for a plain-text consisting of alphabets. However, a number of recently proposed extensions succeeded to encrypt alphanumeric data using different approaches. In this paper, we present another extension for encrypting image content. So, instead of the classical 5*5 matrix, the proposed method constructs 16*16 key matrix for a better alignment with image pixel data. In addition, an XOR procedure has been adopted for a more secure and yet scrambled results. The experimental results showed that the key space of the proposed technique makes it hard for the attacker to perform a frequency analysis based on the used pixel digraphs. Furthermore, further tests showed that a small change in the key value results in completely different cipher-images. PSNR values and histogram comparisons were also deployed to show the robustness of the proposed cipher.

5.2 Future Scope

A few key affectability tests were performed utilizing various close key qualities. Figure 4 (b-f) shows the resultant figure pictures utilizing the key qualities: 21985, 21986, 21987, 21988 and 21989 separately. Figure 5 (b-f) shows the relating remade pictures utilizing increasingly shut faked key worthwhile the correct key is 21987. The outcomes demonstrate that the proposed strategy is touchy to the key. That is, a little difference in the key worth will bring about a totally different picture.

The References

1. A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, Hand-book of applied cryptography (CRC press, 2010)
2. W. Stallings, Cryptography and Network Security: Principles and Practice 5th ed (Pearson, 2011)
3. G.C. Kessler. An overview of cryptography (2003)
4. A. Elhadad, S. Rida, A. Khalifa, DNA-Based Cryptography (LAP LAMBERT Academic Publishing, 2013)
5. Grant. History of the play fair- cipher hanking for history @ONLINE (2013). URL <http://hankingforhistory.com/history-of-the-playfair-cipher/>
6. R.B. K, S.U. Kumar, A.V. Babu, I. Aditya, P. Komuraiah, An Extension to Traditional Playfair Cryptographic Method, International Journal of Computer Applications 17(5), 34 (2011). Published by Foundation of Computer Science
7. M. Sabry, M. Hashem, T. Nazmy, M.E. Khalifa, A DNA and Amino Acids-Based Implementation of Playfair Cipher, IJCSIS) International Journal of Computer Science and Information Security 8(3), 129 (2010)
8. A. Atito, A. Khalifa, S. Rida, DNA-Based Data Encryption and Hiding Using Playfair and Insertion Techniques, Journal of Communications and Computer Engineering 2(3), 44 (2011)
9. S. Hamad, A Novel Implementation of an Extended 8x8 Play-fair Cipher Using Interweaving on DNA-encoded Data, International Journal of Electrical and Computer Engineering (IJECE) 4(1) (2014)

Play-fair

ORIGINALITY REPORT

21 %

SIMILARITY INDEX

6 %

INTERNET SOURCES

7 %

PUBLICATIONS

19 %

STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Bridgeport Student Paper	4 %
2	"Emphasize the Cloud Security Using Various Substitution Techniques", International Journal of Recent Technology and Engineering, 2019 Publication	2 %
3	Submitted to Daffodil International University Student Paper	2 %
4	Submitted to Gulf College Oman Student Paper	2 %
5	Submitted to Kensington College of Business Student Paper	1 %
6	medium.com Internet Source	1 %
7	Submitted to American Intercontinental University Online Student Paper	1 %
8	www.ijarcsse.com Internet Source	1 %

9	Submitted to Pacific University Student Paper	1%
10	Submitted to Study Group Australia Student Paper	1%
11	Submitted to De Montfort University Student Paper	1%
12	grdjournals.com Internet Source	1%
13	Submitted to CSU, Chico Student Paper	1%
14	www.science.gov Internet Source	1%
15	Submitted to Tasman International Academy Student Paper	<1%
16	Submitted to Staffordshire University Student Paper	<1%
17	www.ijert.org Internet Source	<1%
18	Submitted to Leyton Sixth Form College, London Student Paper	<1%
19	arxiv.org Internet Source	<1%

20	Submitted to Bridgepoint Education Student Paper	<1%
21	learncryptography.com Internet Source	<1%
22	Submitted to Athlone Institute of Technology Student Paper	<1%
23	Submitted to CSU, Fullerton Student Paper	<1%
24	Submitted to Higher Education Commission Pakistan Student Paper	<1%
25	uir.unisa.ac.za Internet Source	<1%
26	d-nb.info Internet Source	<1%
27	Submitted to University of Macau Student Paper	<1%
28	Submitted to National Tertiary Education Consortium Student Paper	<1%

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off