Kirkuk University Journal /Scientific Studies (KUJSS)

Volume 15, Issue 1, March 2020 , pp. (18-33)
ISSN: 1992-0849 (Print), 2616-6801 (Online)

Two Stage Text Encryption Using a Private Table of the Sumerian System

Elham Hassan Aziz

Computer System Techniques Department, Institute of Technical – Kirkuk, University of Technical Northern, Kirkuk, Iraq.

ilhamaziz@ntu.edu.iq

Abstract

The massive use of the internet in our contemporary life relates to the increase of the exchange of information through the Internet networks. Due to the importance of the information and to preserve its confidentiality, it protects using theories as well as strategies from attack or abuse.

The aim of the research is to design an algorithm to encrypt text symbols to understandable symbols using private table that contains representation of ASCII of English characters with their suitable Sumerian system numbers. Each letter of the text is converted to ASCII code then encoded as an image using the private table, After that these images are combined together and saved as a new image as a Sumerian image. This image is encrypted first with unintelligible key image that is generated from three external key's (kr, kg, and kb) to be the first stage encryption image. Then the second stage image generates from encrypting the first stage image with another input key image using XOR function which increases image security. The proposed algorithm gives double stage encryption and high degree of security level because of using Sumerian system and using different keys and security methods. Through using the histograms on all tested images, the result image demonstrate the efficiency of the system visually.

Keywords: Image Encryption, Information Security, Text encryption, Sumerian system, ASCII code, XOR.

DOI: http://doi.org/10.32894/kujss.2020.15.1.2

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 15, Issue 1, March 2020 , pp. (18-33)
ISSN: 1992-0849 (Print), 2616-6801 (Online)

تشفير النص على مرحلتين باستخدام جدول خاص بالنظام السومري

الهام حسن عزيز
قسم تقنيات أنظمة الحاسوب، المعهد التقني – كركوك، الجامعة التقنية الشمالية، كركوك، العراق.
ilhamaziz@ntu.edu.iq

الملخص

يرتبط الاستخدام الهائل للإنترنت في حياتنا المعاصرة بزيادة المعلومات المتبادلة من خلال شبكات الإنترنت. نظرًا لأهمية المعلومات والحفاظ على سريتها، يجب حمايتها من الهجوم أو الإساءة باستخدام النظريات والاستراتيجيات.

الهدف من البحث المقدم هو تصميم خوارزمية لتشفير الرموز النصية إلى رموز غير مفهومة باستخدام جدول خاص يحتوي على تمثيل ASCII للحروف الإنجليزية مع ارقام النظام البابلي المناسبة. يتم تحويل كل حرف من النص إلى رمز ASCII ثم تشفيره كصورة باستخدام الجدول الخاص، ويتم دمج هذه الصور معًا وحفظها في صورة جديدة كصورة بابلية. يتم تشفير هذه الصورة أولاً مع صورة مفتاح غير مفهومة يتم إنشاؤها من ثلاثة مفاتيح خارجية (kr و kg و kb) لتكوين صورة التشفير للمرحلة الأولى. يتم إنشاء صورة المرحلة الثانية من تشفير صورة المرحلة الأولى مع صورة أخرى كمفتاح باستخدام وظيفة XOR لزيادة أمان الصورة. أعطت الخوارزمية المقترحة تشفيرًا ثنائي المراحل ودرجة أمان عالية بسبب استخدام النظام البابلي واستخدام مفاتيح واساليب امنية مختلفة. أثبتت الصور الناتجة الكفاءة بصريًا ومن خلال استخدام الرسوم البيانية على جميع الصور التي تم اختبارها.

الكلمات الدالة: تشفير الصور، امنية المعلومات، تشفير النصوص، النظام البابلي، نظام ASCII، XOR.

DOI: http://doi.org/10.32894/kujss.2020.15.1.2

1. Introduction:

The evolution that accompanies the present time in information and communication technologies can be contributed to widening the exchange of information through local and global networks, and as a result of geographical spacing. The exchange of information needs to be protected from intrusion and theft by providing effective ways and modern encryption algorithms.

The encryption process provides the protection of needed information, and this information is not hidden but it can't be read, so anyone can try to open the encryption rely heavily on a well-known and standard algorithm. Therefore, it is necessary to find new methods and algorithms for the purpose of providing privacy and confidentiality needed to save information from penetration [1].

Digital image is a form of information that is transmitted in modern means of communication and the Internet. Therefore, a large level of security is very important in order to preserve its privacy. For this purpose digital images are characterized by a set of characteristics and attributes that allow specific treatments to be performed [2].

System protection is a set of tools and algorithms necessary to protect information and data from external or internal penetration risks. Information protection can be provided in many methods as encrypting or by hiding information and incorporating it in audio or visual media, or using watermarks and other techniques for the preservation of information. The plain text can be encrypted using a cryptographic key, When using same key to encryption and decryption, it is called symmetric encryption, while encryption key differed from decryption key then the encryption is called Asymmetric [3]. The text can be encrypted in more than one way to be a double encryption, Encrypted text can also be hidden in a picture using image manipulations on the image by performing some arithmetic or logical operation.

This paper propose a new algorithm aims to encrypt a text using the Sumerian numeral system [4]. The encryption can be performed as follows: Firstly, save the text in an image, to be a first step to hide the encoded text, secondly encrypt the created image with another new generated color images using XOR method. This gives the encryption process strength and rigidity furthermore, the decoding process is difficult.

2. Literature Review:

A great interest in the subject of text and image encryption has provided a lot of research and studies in order to provide safe methods to keep information safe against theft during the exchange of information through the network. The authors in [5] proposed new method to encrypt the input message, and hiding the encrypted image in cover image by using least significant bit (LSB). In [6] introduce a new algorithm for encryption used multi keys to improving the security by modifying the blowfish method. In [7] a suggestion of a new technique has been proposed as of image steganography inside embedding the encrypted Data file or message using multi algorithms as Hash-LSB with RSA for improving security and data hiding method.

The technique also applied a cryptographic method. another level is to encrypt and decrypt steganography image by using blowfish algorithm and can used as complementary methods of encryption while exchange of private data. The focus of the research [8] deals with a new dual steganography technique with an additional steps of security. The algorithm included a secret text message in the cover image in three stages. First using vigenere cipher to encrypts the secret message then it uses whitespace text steganography technique, finally using LSB image steganography technique to hides the cover text in cover image. At the end, Stego-image appears completely intact and unwanted person cannot aware of a secret message inside the cover image

3. Information Security System:

The widespread use of information through multimedia and computer networks makes the information protection system an important topic. There are different method to protects data such as encryption or steganograghy and watermarks see Fig. 1 [3].

Encryption is a process to change the form of Plain text to the Cipher text using mathematical equations and the existence of a key that is used in the process of encryption and decryption. There are two types of encryption, the first is One - key encryption (Symmetric), which uses the same key for both encryption and decryption process. The second encryption type is the public key encryption that uses two keys (Asymmetric) [9].

.

Steganography is a technique of data hiding within the Digital media (text files, video files, audio, or e-mail messages) [9] as showen in Fig. 2. The use of steganography can be combined with encryption as an additional step for hiding or protecting data Fig. 2. The secret key is a knowledge that agreed between the sender of the message and the recipient, making the process of hiding complex [9].

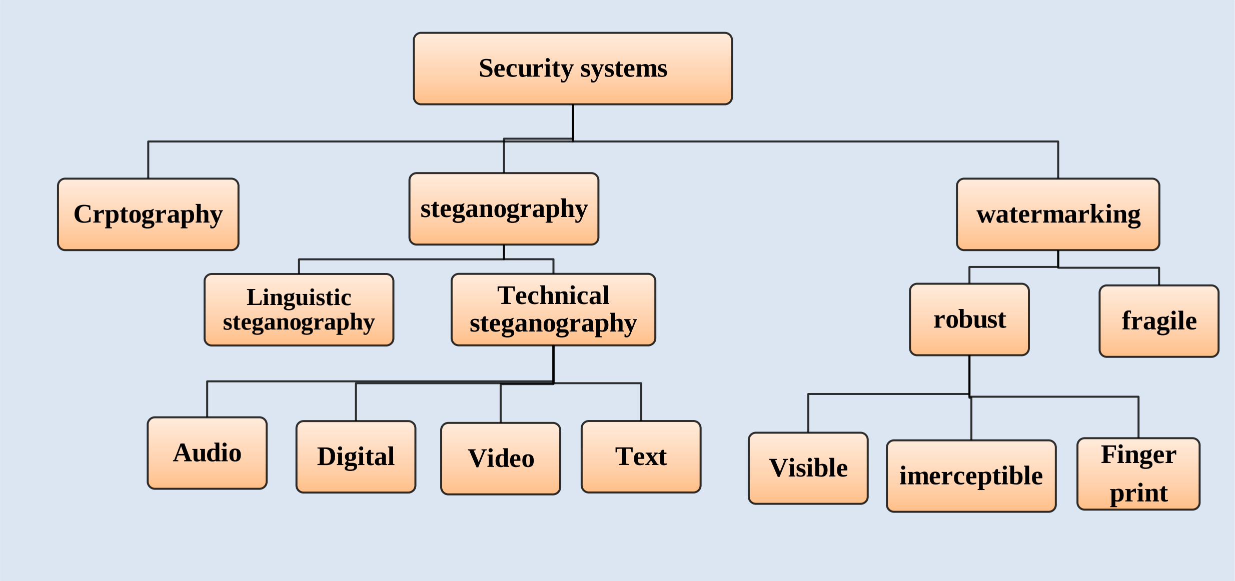


Fig. 1: Data protection system [14].

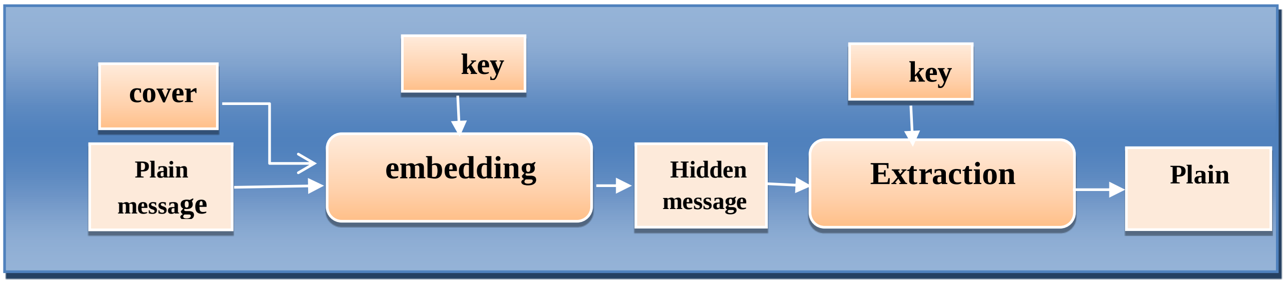


Fig. 2: Hiding scheme [15].

The color image is defined as a three dimensional digital image of size (MxNx3) where each pixel (or point) in the image consists of three colors RGB (red, green and blue), and each of them takes 8 bits, so that the color image will take 24 bits per pixel, each color takes (0-255) to represent the probability of light to dark. The total probability of color values (2^{24}) per pixel. The color image has two important qualities.

The first is the colors which it can extract and process some concepts in the components of the image, the second is thousands of color gradients and its intensity that human can distinguish and recognize which is important in images analysis and processing [10] [11].

Digital image can be analyzed through image processing using different methods to obtain attributes of the image. Basic processing can be done to the image such as: resize, crop or rotate and the arithmetic and logical image processing. Also image can be analyzed by computer vision, that allows high levels of extraction of image information such as color and attributes [10].

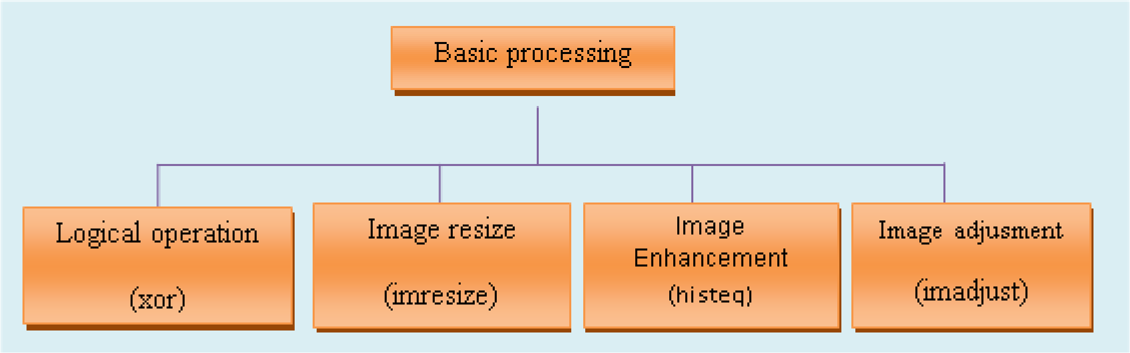


Fig. 3: Pre-processing.

Encoding in computer science is defined as the process of transforms data into a specialized format by using a scheme that is mostly available So it can be easily reversed. The key is not required because the conversion of an encoded format back into the original sequence of characters by reverse encoding. The process of converting encoding data into plain text is called decoding [1].

4. The Sumerian Numbering System:

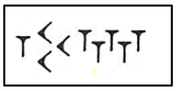
In most of the world nowadays, the Decimal system is a worldwide numbering system that uses the Hindu-Arabic digits 0-9 are used. The value of the Decimal number is affected by the position of these digits. The given a positional system needs a convention concerning which end of the number represents the units. For an example the Decimal number 12345 is represented as: $1 \times 10^4 + 2 \times 10^3 + 3 \times 10^2 + 4 \times 10^1 + 5\times 10^0$.

The Sumerians developed the earliest known writing system, their numerical system is one of the oldest numerical systems used by humans as painted symbols on clay boards.

Sumerians used the Sexagisimal system (base of 60). The Sumerians established system was incomplete in the sense that they used positional notation only in base 60, (1,10,60, 600,3600) [12].

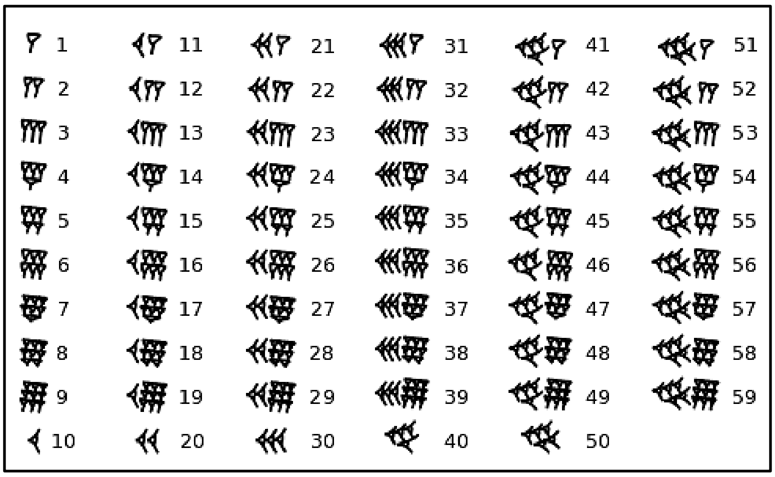
This system improved to use only two symbols: a pin shape } (represents the value one), and wing shape (represents the value 10). These two symbols could represent different numbers based on their position. Numbers under 60 were written from 1 to 59 as shown in Table 1.

The Sumerian number system is read from left to right, so the number 95, as an example, was as follows:



The first pin represents the value 60, the three wings are equals to 30 (3 X 10), and the final five pins are equals to 5 (5 X 1), that give 95 as total [13].

Table 1: The Sumerian 59 symbols [13]



1	11	21	31	41	51
2	12	22	32	42	52
3	13	23	33	43	53
4	14	24	34	44	54
5	15	25	35	45	55
6	16	26	36	46	56
7	17	27	37	47	57
8	18	28	38	48	58
9	19	29	39	49	59
10	20	30	40	50	

The symbols used for representing any long numbers in Sumerian system are a combination of: symbols in place one's (1-9), symbols in place of ten's (10, 20, …100), symbols in place of sixty's and symbols in place of (60x60) and so on, as declared in tables (2 and 3). Instead of using the zero between the number's symbols, an empty column is leaved between them, and extra space is leaved to separate between the numbers [13].

Table 2: Decimal numbers with their related Sumerian symbols [4].

Decimal Number	Sumerian Number	Decimal Number	Sumerian Number
1	𒁹	10	𒌋
2	𒈫	20	𒎙
3	𒐈	30	𒌍
4	𒐉	40	𒐏
5	𒐊	50	𒐐
6	𒐋	60	𒁹
7	𒐌	70	𒁹 𒌋
8	𒐍	80	𒁹 𒎙
9	𒐎	90	𒁹 𒌍

For example, the letter (M) corresponds to the ASCII code is equal to (77) is represented in Sumerian system as a combination of the three numbers (60+10+7), that the number 7 is at place one's, 10 is at place ten's, and 60 is at place 100's. The ASCII code of the letter J is (74) which can be represented as (60+10+4), and so on, as shown in the following examples [4]:

77 = 60+10+7 = 𒁹 + 𒌋 + 𒐌

74 = 60+10+4 = 𒁹 + 𒌋 + 𒐉

6 = 0+ 0 +6 = □ + □ + 𒁹

60 = 0+60+0 = □ + 𒁹 + □

The examples listed in Table 4 shows the representation of some English characters using the Sumerian system.

Table 3: Decimal numbers Representation with Base 60 numbers[4].

Number	First	Second x60	Third x 3600
1	𒐕		
10	𒌋		
60		𒐕	
61	𒐕	𒐕	
3600(60x60)			𒐕

Table 4: Examples of Sumerian numbering system related to some English letters [4].

Character	ASCII Code	Picture of Sumerian No.			Combined Picture of Sumerian no	Character	ASCII Code	Picture Sumerian no.			Numerical Sumerian no.
M	77	𒐕	𒌋	𒐛	𒐕 𒌋𒐛	J	74	𒐕	𒌋	𒐘	𒐕 𒌋 𒐘
N	78	𒐕	𒌋	𒐜	𒐕 𒌋𒐜	K	75	𒐕	𒌋	𒐙	𒐕 𒌋 𒐙
O	79	𒐕	𒌋	𒐝	𒐕 𒌋𒐝	L	76	𒐕	𒌋	𒐚	𒐕 𒌋𒐚
P	80	𒐕	𒎙		𒐕 𒎙	k	107	𒐕	𒐏	𒐛	𒐕 𒐏𒐛

5. The Proposed Text Encryption Algorithm:

In this research, the explicit text is encrypted using Sumerian numbering system, It uses Base 60 numbering system as mentioned above. The plain massage in English characters are converted first to the corresponding ASCII code.

This code number is encrypted by using its equivalent symbol in Sumerian system that shown in Tables 1 & 2 as a small images of size (30x30) pixel. Because of ASCII numbers for any printed character is <= 128, all needed Sumerian symbols for these codes are 128 ASCII symbols. These symbols are previously stored in a private table.

From this table a matrix known Sumerian matrix is created to contain these Sumerian symbols as small images sequentially with index equals the ASCII code of the symbol.

All ASCII codes of the plain text characters are converted to its corresponding Sumerian symbols using the private table (Sumerian matrix), then saved sequentially into a new prepared image to get the source image (Sumerian image). The Sumerian image is prepared to have 12 letters in each row, so each row will have length equals to (12 symbol * size of each small image) as shown in Fig. 5a, so the image size will depend on the length of the input plain text.

Another image is prepared and generated for the first stage encryption using three different external keys (k_r, k_g, k_b). Each key is used as a starting value to fill the key image with colors (RGB), each of these colors will be increased sequentially by A certain number to get the pixel's colors of the key image (key1) Fig. 5b. This key image is used to encrypt the Sumerian image with XOR function as a first stage of the encryption Fig. 5c.

The second stage of encryption is done on the resulted image of the first stage with a new loaded image (key2) Fig. 5d which is stretched to fit the size of the Sumerian image, this encryption is done using XOR method to obtain the second stage image or Cipher image Fig. 5e. The proposed encryption steps are listed in the algorithm.

The first decryption starts with decrypting the second stage image using (key2), to retrieve the first stage image. The second decryption is applied on the first stage image with (key1) image that generated from the same keys (k_r, k_g, k_b) used in the encryption process to get the source (Sumerian image).

Finally split the symbols from last obtained image to get the Sumerian symbols, these symbols are matched with images in the private Sumerian matrix to get their indexes that represents the ASCII code of the English characters that lead to the plain text back. The decryption steps are listed in the algorithm.

The proposed Algorithm:

1- Encryption steps of the Algorithm

step 1. Begin

step 2. Enter the explicit plain text to be sent in English.

step 3. Find (ASCII) code for each letter of the plain text.

step 4. Get the Sumerian symbol for each ASCII number from the Sumerian matrix indexes.

step 5. Save all Sumerian symbols from step 4 into a new source image (Sumerian image).

step 6. Enter the keys (k_r, k_g, k_b).

step 7. Generate the key image (key1) using the above keys as starting colors for it.

step 8. Encrypt the Sumerian image from step 5 with (key1) to get first stage image using XOR function.

step 9. Load an image as a key image(key2) for the second stage encryption.

step 10.Stretch the image (key2) to fit the size of the first stage image.

step 11. Encrypt the first stage image with (key2) to get the second stage image (Cipher image) using XOR function.

step 12.Send the final encrypted image (Cipher image).

2-Dencryption steps of the Algorithm

step 1. Load The Encrypted image (Cipher) that contain the encrypted text.

step 2. Load the key image (key2)

step 3. Decrypt the Cipher image (second stage image) with key2 (stage2)

step 4. Enter the keys (k_r, k_g, k_b)

step 5. Generate the key image (key1) using the three keys.

step 6. Decrypt the image stage2 to get stage1 image using (key1) to get the Sumerian image (using XOR function).

step 7. Split stage1 image (Sumerian image) to small images (each three of them as one symbol).

step 8. Search the Sumerian symbols in the Sumerian matrix images and get their indexes (the ASCII code).

step 9. Convert ASCII code to the corresponding English characters.

step 10.Combine the characters to get back the plain text

step 11.End.

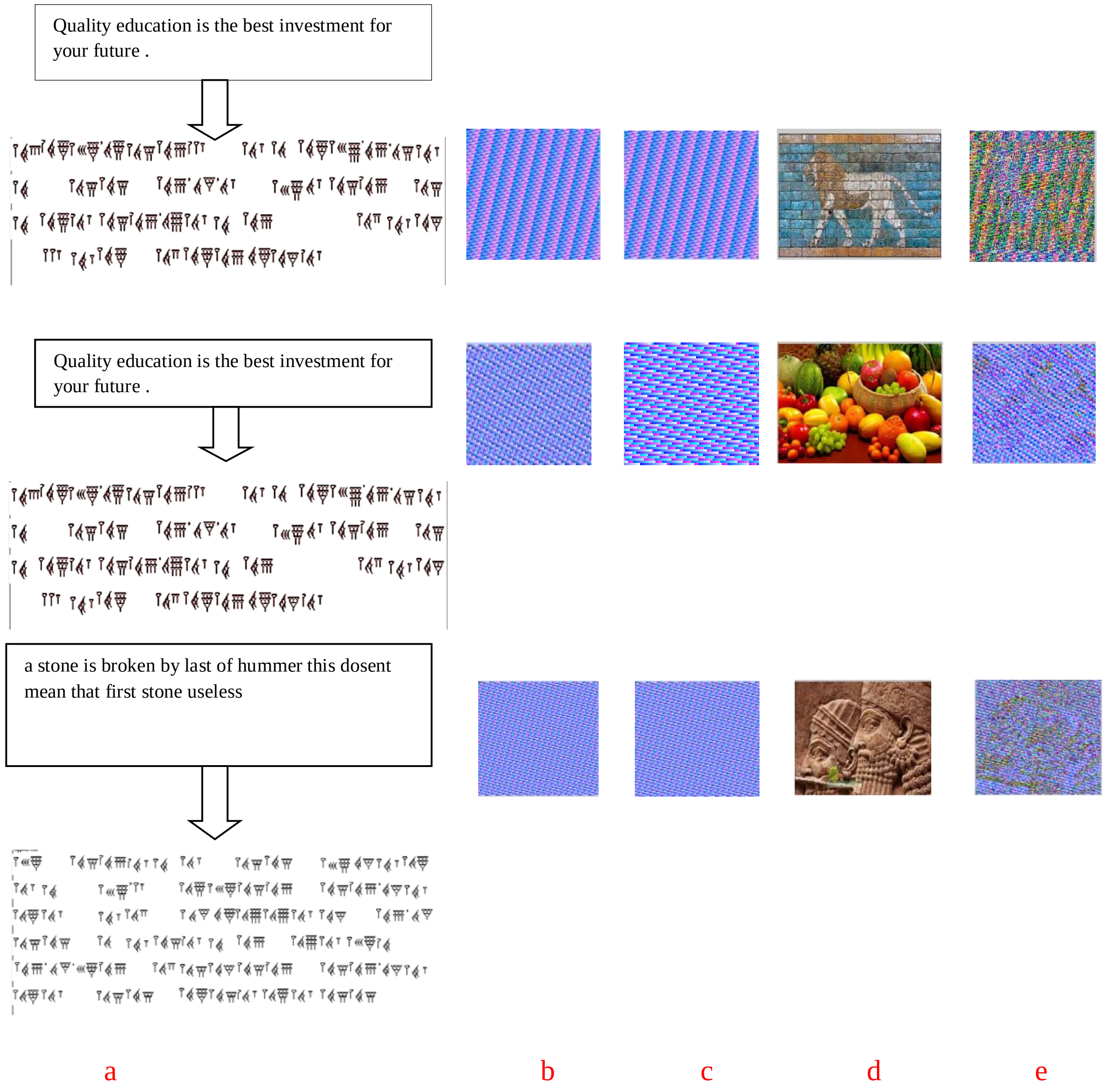

Quality education is the best investment for your future .
Quality education is the best investment for your future .
a stone is broken by last of hummer this dosent mean that first stone useless
a
b
c
d
e

Fig. 5 : Images of encryption

a. Explicit-text with Sumerian text (source image)

b. key image (key1)

c. First stage encrypted image

d. Key image (key2)

e. Second stage or Cipher image

6. Results and Discussion:

In the proposed system, the plain text is converted first to Sumerian symbols shown in Fig. 6 a which is vague to many people's.

The first stage image resulted from encrypting the Sumerian image by a triple keys (k_r, k_g, k_b) that shown in Fig. 6c, is visually unintelligible image and it is hard to break. Histogram is a graphical form used to show distribution for each color band of the image. horizontal axis shows colors proportion, while the vertical axis shows the final value of these colors appearance. All resulted images are tested using histograms in MATLAB program.

The histogram of the first stage image in Fig. 6b shows a low correlation between its pixels that provided good level of security. The second stage image resulted from the second encryption gave another security to the system.

As shown in its histogram Fig. 6d, low correlation and differs from the first histogram in Fig. 6b. The last encrypted image (Cipher image) completely different from the source image (Sumerian image) and that is very clear in the shown histogram in Fig. 6f.

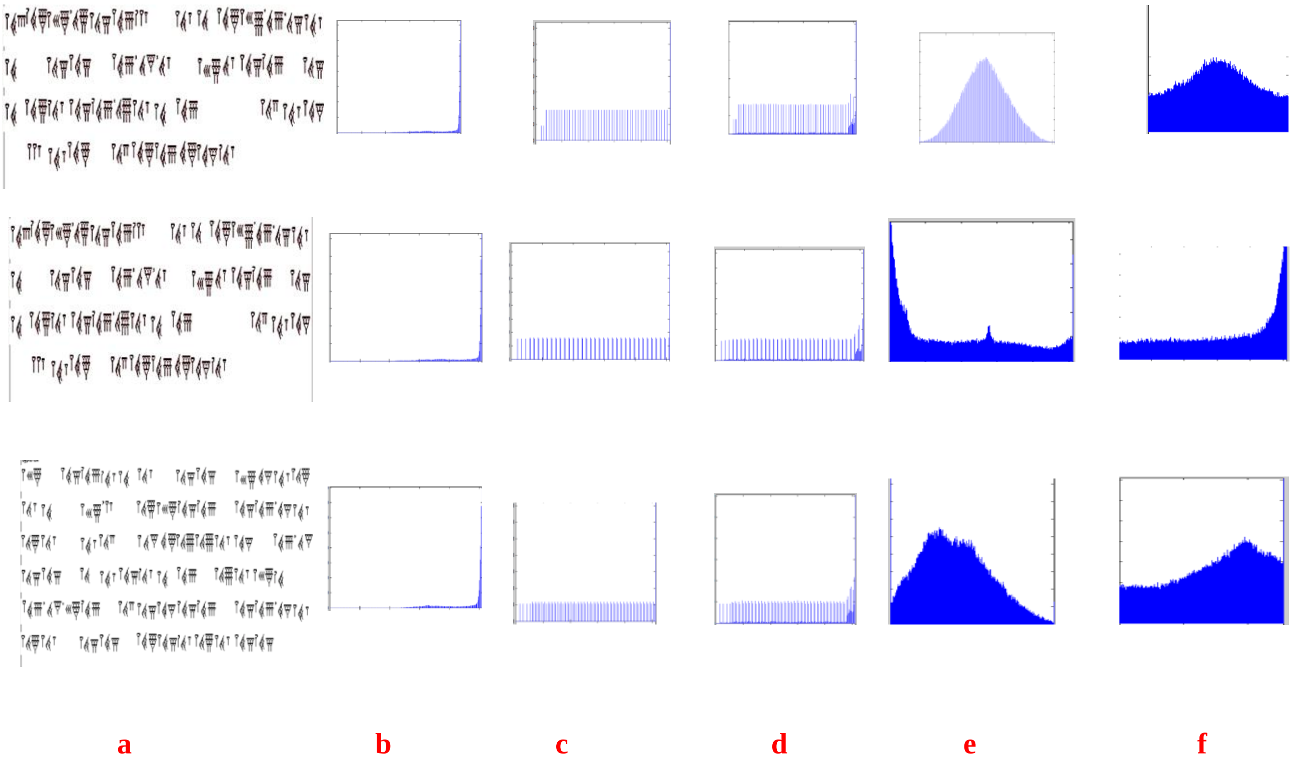


Fig. 6 : Testing Images Histogram

a. Cipher text in Sumerian symbols

b. Histogram of Cipher-text

c. Histogram first stage image (key1)

d. Histogram of first stage encrypted image

e. Histogram Second stage or Cipher image (key2)

f. Histogram of Cipher image

7. Conclusions:

This paper proposed two stage encryption system, it gets its secrecy from using the Sumerian numbering system that is vague and unknown to most people. The diversity of the encryption methods made the process to guess or get back the text again so hard. Firstly, because it is saved as an image not as characters and without using the traditional ways in the encryption, secondly the attacker must know the Sumerian numbering system and its algorithm for text and numeric representation in order to obtain the corresponding English message. Thirdly the use of the external three keys (k_r, k_g, k_b) that must be guessed, and the attacker must find the way to use them in the generation of the key image (key1). Lastly , the additional security provided by second stage encryption using loaded image (key2). All these reasons made the operation of braking the Cipher image confusing process. Finally The proposed method was highly secured in its results, the encrypted images shown in tested results were visually unintelligible and all histograms proved the efficiency of the system.

References:

[1] V.K Pachghare , "***Cryptography And Information Security***", 2nd Ed. , publisher PHI learning private limited, delhi ,Indian, 2 (2015).

[2] Anurag Singh and Namrata Dr.Dhanda," ***Dip Using Image Encryption And Xor Operation Affine Transform*** ", IOSr journal of computer engineering , 17(2), (2015).

[3] Peter Wayner ," ***disappearing cryptography information hiding steganography & watermarking*** ", 3rd Ed. , publisher Morgan Kanfmann in elsevier Inc , USA , 1 (2009).

[4] Elham H. A. and Wafa M. J. "***Design Adaptive Encryption Algorithm By using Sumerian Numbers***", Krikuk University Journal (KUJSS), 12(3), (2017).

[5] ,Aymen Mudheher Badra and al, " ***Image in Image Steganography based on modified Advanced Encryption Standard and Lest Significant Bit Algorithms***", journal of university of babylon for pure applied and sciences, 26(8), 112 (2018).

[6] Nada Hussein, M. Ali and Suaad Ali Abead," ***Modified Blowfish Algorithm for Image Encryption using Multi Keys based on five Sboxes***", Iraqi journals of science, 57(4C), 2968 (2016).

[7] M. Rajkamalp , B. S. E. Zoraidap ," ***Image and Text Hiding using RSA & Blowfish Algorithms with Hash-Lsb Technique*** " , International Journal of Innovative Science, Engineering & Technology(IJISET) , 1(6), 81 (2014).

[8] Priti Sehgal and el," ***Hiding Encrypted Text Using Text And Image Steganography: A Dual Steganographic Technique*", International Journal Of Electrical, Electronics And Data Communication, 5(7), 54 (2017).

[9] A.joshi,madhuri ," ***Digital Image Processing an Algorithm***", 3rd Ed. , publisher PHI learning private limited, delhi, india ,376 (2018).

[10] C. Rafael Gonzales, E. Richard Woods, "***Digitial Image Processing***", 3rd Ed. ,PHI learning private limited, delhi ,Indian, 394 (2008).

[11] C. Rafael Gonzales and al," ***digtail image Processing Using Matlab*** " , 2nd Ed., gatesmark publishing ,www.gatemark.com,printed in USA, 13(2009).

[12] T. Zara, "***Sumerian Mathematics***", A Senior Thesis , Liberty University, USA(2008).

[13] J. J. O'Connor and E. F. Robertson, "***Sumerian numerals***", Mac Tutor History of Mathematics School s ,University of St Andrews, Scotland , (2000).

[14] Ahmed Hussain and el," ***Enhancing The Hiding Capacity Of Audio Steganography Based On Block Mapping***", Journal of Theoretical and Applied Information Technology, 95(7), 1441 (2017).

[15] M. Gajalakshmi, R. Vidya ," ***Review on - Data Hiding using Cryptography and Steganography***", International Journal of Computing Algorithm, 7(1), 25 (2018).