Volume 4, Issue 11, November 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Keys Constructing

Ali Abdul Azeez Mohammad Baker, Zainalabideen Abdullasamd Rasheed
Education College,
Kufa University, Iraq

Abstract—Security is one of the most important things in current era because of danger effects of extracting secure information by any unwanted part where information is critical and effective. There are many methods applied to ensure information security like steganography, cryptography, biometrics, barcodes, and passwords, all these methods have different levels of security and have strong and/or weak features in different cases. cryptography provide strong method for keeping information secured and undiscovered from unwanted persons, and this state depends on some parameters like method complexity, key length, key randomness, and key security. In this paper a new method will be suggested to construct secure and randomness keys and avoiding the problems of changing and sending keys between authorized parts. The proposed method constructing fifteenth digit key from colored image by discovering sixteen digits from each band through extracting the essential repetitive colors and two digits from the size of the image. the most important feature of this key that it can be reconstructed in all authorized parts that received the specific image in spite of changing could be happened through channel in the networks that will be used in sending secure information from one part to all other authorized parts.

Key words— Cryptography, Symmetric key, Normalization, Vigenere algorithm, monoalphabetic.

I. INTRODUCTION

Cryptography is the science of hiding information-meaning, or is an essential tool for the protection of important information. The goal of cryptography is to make data unreadable by unwanted persons. Cryptography algorithms can be divided into two types according to the key that will be used in ciphering algorithm, secret- key (symmetric) and public-key (asymmetric) algorithms, Symmetric algorithms are used to encrypt and decrypt plaintext by using the same key in both algorithms. However Public-key algorithms use pair of keys, one of them is used in encryption information that will be sent to a receiver (public) who owns the corresponding private key which is used in decryption process.

There are many symmetric encryption algorithms, which can be divided into monoalphabetic (like Caesar method) and polyalphabetic substitution algorithms (like Vigenere method), the second type is more secure and more important than the first.

Vigenere algorithm used symmetric key that that will be repeated until plaintext length, then ciphering each digit or letter according to the key letter alphabet and then inverse process will be applied in decipher cipher text. For example if the plain text is (kufa university) and key is (edu), the cipher text becomes (oxzexhmyyvvcxb) as illustrated in figure (1)

k	u	f	a	u	n	i	v	e	r	s	i	t	y
e	d	u	e	d	u	e	d	u	e	d	u	e	d

a- key repetition

Plain→		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
key	e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
	d	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
	u	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t

b- cipher method

Fig. (1) Vigenere algorithm

II. THE PROPOSED SYSTEM

The proposed system consist of many steps as illustrated in figure (2)

A. Normalization:- this step will be applied on each band of the colored image by applying the following steps

- Dividing each one of them into four quadruple firstly.
- Calculating four essential colors for each part which are depend only on two MSB.
- Calculating number of pixels for each essential color for each band.
- Calculate the maximum and minimum numbers.
- Normalized the results by applying the following formula

$$KD = 1 + \text{int}(25 * \frac{Pn - \min}{\max - \min})$$

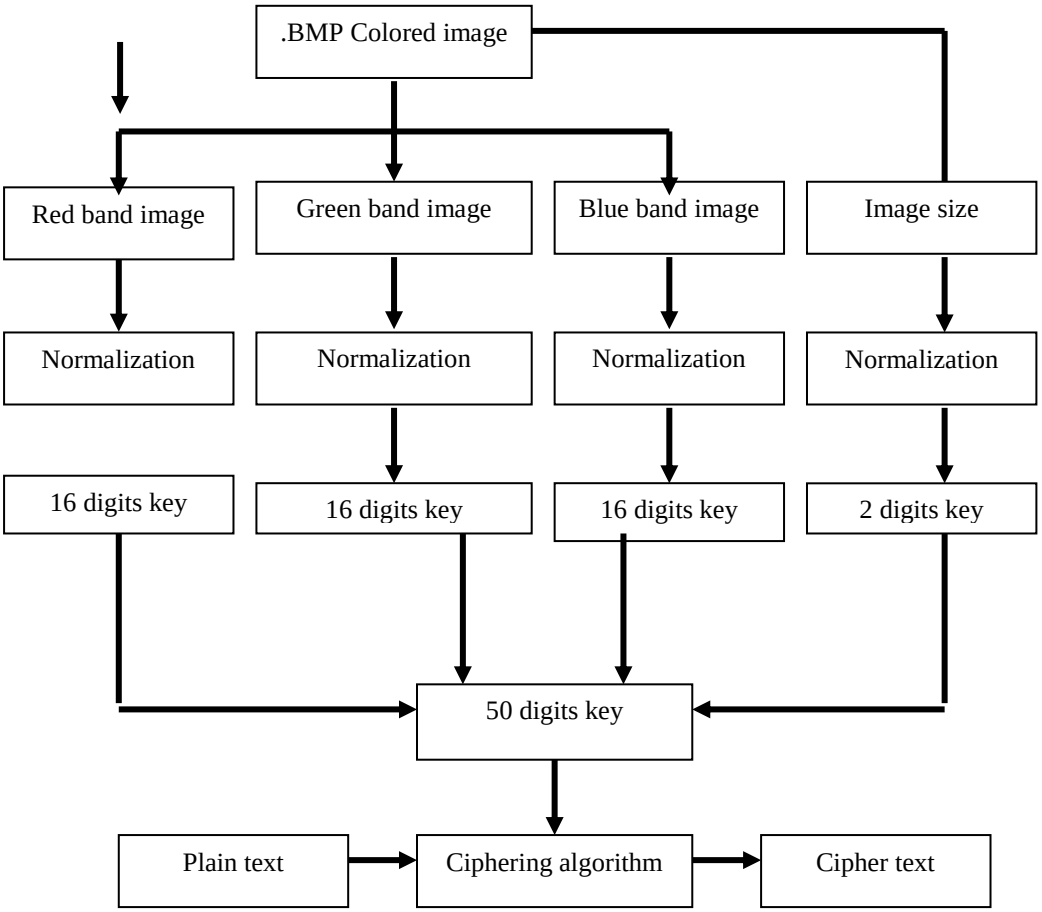


Fig. (2) the block diagram of the proposed system

The steps of the proposed system can be illustrated by the following explaining

(1)

Where,

KD is key digit
Pn is pixel number
Max is maximum pixels number
Min is minimum pixels number

The number (Pn) is usually still and unchangeable because is depend on two MSBs on the right representation of binary format of eight bits, that is mean is maintain from changing through sending within networks even some pixel values are change but practical will be proven that two of MSBs are still same after compressing or filtering noise.

This step will be applied on image size by applying the following formula

$$KD = 1 + (w/h) \bmod 26 \quad \ldots$$

(2)

Where,

KD is key digit
W is image width
H is image height

These steps can be illustrated in figure (3) and table (1) below

Fig. (3) colored image

After applying the normalization step on each band the following table can be calculated

TABLE (1). SECURE KEY CORRESPONDING TO COLORED IMAGE IN FIGURE (3)

	color	Red band	Green band	Blue band	Key related to red	Key related to green	Key related to blur
First part	00	8	8	6	H	H	F
	01	4	5	2	D	E	B
	10	12	14	6	L	N	F
	11	17	14	26	Q	N	Z
Second part	00	21	20	11	U	T	K
	01	10	12	12	J	L	L
	10	8	7	12	H	G	L
	11	2	1	6	B	A	F
Third part	00	10	9	7	J	I	G
	01	4	6	4	D	F	D
	10	8	10	5	H	J	E
	11	19	16	24	S	P	X
Forth part	00	22	25	17	V	Y	Q
	01	10	10	9	J	J	I
	10	7	5	11	G	E	K
	11	1	1	4	A	A	D

The two additional digit will be calculated as below by applying equation (2)

KD(49)= 65+ (255 mod 26) = 86≡V

KD(50)= 65+ (383 mod 26) = 84 ≡T

So the key related to image in figure (2) is

HDLQUJHBJDHSVJGAHENNTLGAIFJPYJEAFBFZKLLFGDEXQIKDVT

B. Ciphering algorithm:- the ciphering algorithm depend on simple modified to Vigenere algorithm as follows

- The text will be ciphered with the secure key by applying Vigenere algorithm.
- Repeat above step to re-cipher the ciphered text with the same key by applying Vigenere algorithm too.

This algorithm can be illustrated by the following simple example

Plain text is KUFA

Key is AMSI

plaintext	key	First cipher step	cipher text
K	A	K	K
U	M	G	S
F	S	X	p
A	I	I	Q

III. RESULTS

the following results can be obtained when the proposed system will be applied on sampled images as follows

Example1:

Fig. (4) image used in constructing key

Extracted key: XDAAXEAAZCAAWEAAQEFALEMAUDDAPEHAQCGBKBJGUCEAOCGDV

Plaintext: ALI ABDUL AZEEZ MOHAMMAD BAKER AL QAZZAZ

Ciphered text: URIAVLULYDEERUOHGUWAZJYKSXGLUINZGD

Example2:

Fig. (5) image2 used in constructing key

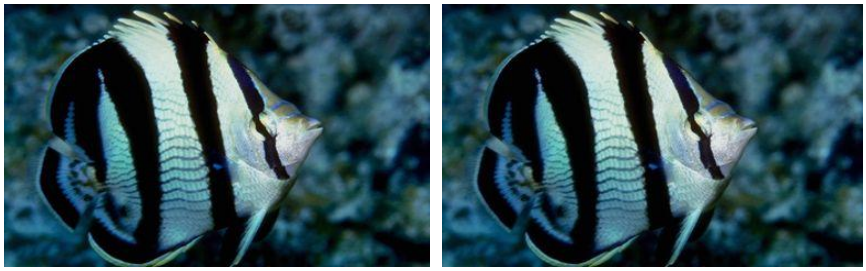
Extracted key: QHCEQJEBLNECMJIASGBERJDBNNBCOLEAXBCCZDDAXEBBYGAAT
QHCEQJEBLNECMJIASGBERJDBNNBCOLEAXBCCZDDAXEBBYGAAT
Plain text: ZAIN ABDUL SAMAD
Ciphered text: FOMVGTLWHSIQYV
Example3:

Fig. (6) image3 used in constructing key

Extracted key: NLGARFFDZECARJGATGFBSEHDYECBUHFAJPDEKHNCKQECOLGAT
Plain text: COMPUTER SCIENCE EDUCATION COLLEGE KUFA UNIVERSITY
Ciphered text: CKYPCDOXRAGIMFOEQPEEKBWUJKSNZSQECYLIOBIZYXAMVU

IV. CONCLUSIONS

- The proposed system is very useful in term of sending images through networking area where images compressed in loose algorithm, The same key will be retrieved after applying loose algorithm for compression as illustrated in figure (7).

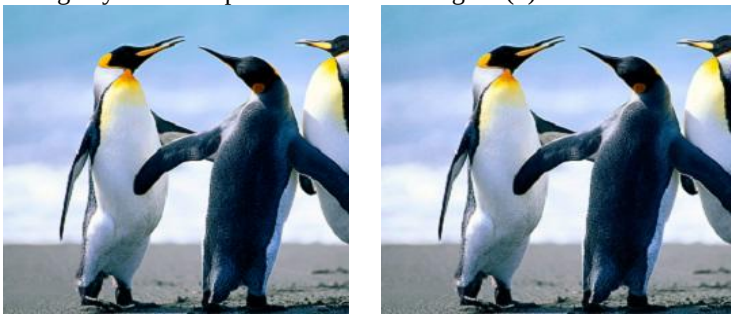


a- original image (bmp) b- .Jpeg image

Fig. (7) positive effect of compression on constructing key

Extracted key from bmp image: QHCEQJEBLNECMJIASGBERJDBNNBCOLEAXBCCZDDAXEBBYGAAT
Extracted key from jpeg image: QHCEQJEBLNECMJIASGBERJDBNNBCOLEAXBCCZDDAXEBBYGAAT

- Some images constructing keys with simple difference as in figure (8)



a- original image (bmp) b- .Jpeg image

Fig. (8) negative effect of compression on constructing key

Extracted key from bmp image: BAAZKEHFEDATBCMKBANMMDHEFBGNCDNIBDQFNDFEGBOFDELIV

Extracted key from jpeg image: BAAZKEHFEDBTBCMKBANMMDHEFBGNCDNIBDRFNDFEGBOFDELIV

As shown in figure (8), some letters of the public key in generating process could be effected due to some changing which be happened to the image through channels and is so small and non-effective because the whole meaning can be predicated.

- The randomness degree of the constructing key is very good and there are no repetitions of specific letters in the key.

REFERENCES

[1] Nesir Rasool Mahmood, Ali Abdul Azeez, and Zahraa Nesir Rasool " Public Key Steganography", International Journal of Computer Applications, Volume 100– No.8,USA, August 2014.

[2] Shahana T "A Secure DCT Image Steganography based on Public-Key Cryptography ", India, 2013.

[3] Minati Mishra, Priyadarsini Mishra, M.C. Adhikary and Sunit Kumar," IMAGE ENCRYPTION USING FIBONACCI-LUCAS TRANSFORMATION", IJCIS, India, 2012.

[4] Rajinder Kaur, Er.Kanwalprit Singh " Image Encryption Techniques:A Selected Review", IOSR-JCE, India, 2013.

[5] Yahya Alqahtani, Prakash Kuppuswamy, and Sikandhar Shah " NEW APPROACH OF ARABIC ENCRYPTION/DECRYPTION TECHNIQUE USING VIGENERE CIPHER ON MOD 39", International Journal of Advanced Research in IT and Engineering, 2013.

[6] Massoud Sokouti, Babak Sokouti, Saeid Pashazadeh and Leili Mohammad Khanli " FPGA implementation of improved version of the Vigenere cipher", Indian Journal of Science and Technology, Iran,2010.

[7] E. Anupriya et al. " Encryption using XOR based Extended Key for Information Security – A Novel Approach", International Journal on Computer Science and Engineering (IJCSE), India,2011.

About Author

Ali Adul Azeez Mohammad Baker University of Kufa, Education College, Najaf, IRAQ. He received BSc in computer sciences (2010), civil engineering (1990), and MSc in computer sciences (2012), worked as a teacher in Kufa University, has many published papers. His research interests are in image processing, and security (biometrics, and steganography), He's Associate teacher in Computer Science at the University of Kufa – Najaf, IRAQ. E-mail: alia.qazzaz@uokufa.edu.iq, Tel: +964-7803369309.

Zainalabideen Abdullasamd Rasheed University of kufa, Education of College, Najaf /Iraq. Has a BSc (Baghdad University, Iraq), and MSc (Buckingham university, United).he has a long experience in teaching various computing practical courses at Baghdad university .at AL Kufa university, Mr Rasheed teaches different courses like computer organization, operating system and computer architecture .he supervises undergraduate projects. He interest in data security (steganography and cryptography) and digital image processing (biomedical image and edge detection, de-noising images).E-mail: zain9999@live.com, Tel: 009647711131246 .Iraq.

