A Steganographic Approach to Data Obfuscation using Random Keyboard Mapping Technique

Kaustab Pal
University of Engineering and Management
UEM,Gurukul,Udaipuria Mod,Chomu,Jaipur,Rajasthan

Rupayan Das
University of Engineering and Management
UEM,Gurukul,Udaipuria Mod,Chomu,Jaipur,Rajasthan

Rahul Sourav Singh
University of Engineering and Management
UEM,Gurukul,Udaipuria Mod,Chomu,Jaipur,Rajasthan

Dipta Mukherjee
University of Engineering and Management
UEM,Gurukul,Udaipuria Mod,Chomu,Jaipur,Rajasthan

ABSTRACT

This paper proposes a hybrid approach to enhanced data security using special matrices in conjunction with Steganography. The special matrices are used for mapping the actual characters to numbers which are actually pointers to the location of the characters in the matrices. The generated numbers corresponding to each character of the message are embedded in the image pixels at the least significant bit position prior to transmission. The change of LSB values of the image pixels do not distort the image significantly, allowing for undetected transmission of any message to its intended receiver.

Keywords

Cryptography; LSB; Steganography;

1. INTRODUCTION

Just as the Industrial Revolution has marked the onset of the Industrial age; the onset of the Information age has been associated with the Digital Revolution. Data security, in the modern world is an inherent part of our lives. It is achieved by various techniques such as passwords, cryptography[6], bio-metrics, Steganography and other such techniques [1]. The increasing development of digital information sharing through networking has pushed the world towards adopting new methods and techniques for protecting and hiding digital data through cryptography and Steganography. In cryptography [2], secret data are converted into unreadable and obscure data by one or more cryptographic keys and its main goal is to hide contents of a secret message and not necessarily communication itself. Normally encrypted messages usually attract hostile attention and are prone to sabotage. To address this problem, Steganography can be used in addition to cryptography. The main aim is to camouflage the secret communication as well as the medium of sending the message itself by putting the confidential data in a cover media, generally images, so that the very existence of the hidden message can't be detected or even predicted. In this paper we propose an algorithm that implements both the concept of Steganography and cryptography to obscure and conceal our message. The proposed algorithm focuses on encrypting the message in a randomly generated character matrix and the key so generated is then hidden in an image using pixel LSB replacement technique. The resulting image thus produced has less distortion and the message is transmitted securely without any detection.

2. PROPOSED ALGORITHM

2.1 Methodology

The proposed algorithm employs a matrix pool containing 20 randomly created keyboard matrices. Each matrix is one dimensional and each and every matrix has a unique character position. Data is mapped on a randomly selected matrix and the position of the characters on the matrix acts as the key. Each bit of the key is then embedded on the least significant bit positions of the image pixels. Due to changes in the LSB, the image does not distort significantly and a high signal to noise ratio is obtained resulting in an undetected transmission of the message.

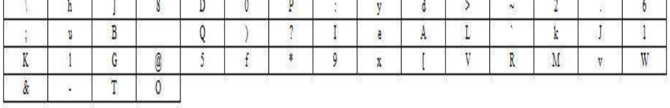
During the encryption process, a random matrix is selected from the matrix pool and the matrix number is taken as key 1. The length of the plain text gives us key 2 and the characters of the plain text is then compared with the characters of the selected matrix and when found, their positions are stored as a key 3. All the three keys are then converted to their equivalent 7 bit binary and each bit is then embedded into the LSB of the pixel values of the image and the stego image is obtained.

During the decryption process, the LSB of the first seven pixel values of the stego image gives us key 1 which is the matrix number which is then selected from the pool. The LSB of the next seven pixel values gives us key 2 which is the length of the plain text. The next pixel values up to the length of the plain text gives us the positions of the characters in the matrix, i.e. key 3. The characters are then extracted from the chosen matrix and the plain text is obtained.

2.2 Implementation

Matrix Pool: 20x1D matrices each containing the same characters but in a unique position in every matrix.

Matrices: The contents of the matrices are as follows



}	^	F	E	%	(	Y	=	$	H	|	q	/	U	!
X	#	w	z	"	g	_	S	j	t	Z	7	b	p	s
N	c	3	n	<	C	,	+	m	r	a	i	4	{	o
\	h	]	8	D	0	P	:	y	d	>	~	2	.	6
;	u	B		Q	)	?	I	e	A	L	`	k	J	l
K	1	G	@	5	f	*	9	x	[	V	R	M	v	W
&	-	T	O											

Fig-1: Table 1 Matrix 1

]	q	$	i	t	}	0	1	*	;	?	D	g	X	:
4	[	.	<	>	Q	=	Z	|	m	!	e	@	R	7
j	k	K	%	F	#	b	c	9	P	C	o	v		)
M	O	n	U	w	y	h	u	N	3	\	`	s	^	"
&	(	Y	6	J	V	{	5	x	-	8	d	W	/	z
L	G	a	_	r	B	H	I	p	T	S	~	E	2	A
1	f	+	,											

Fig-2:Table 2 Matrix 2

z	0	{	T	)	7	f	<	h	~	=	U	d	}	g
5	C	N	i	s	n	x	&	V	e	!	E	$	6	p
,	H	(	D	o	9	[	.	8	Y	#	+	a	1	u
2	?	>	A	F		b	I	%	O	R	;	q	"	S
P	t	`	v	j	*	/	L	Q	G	K	^	W	m	l
-	4	w	c	B	k	X	@	\	y	|	r	M	J	]
_	3	:	Z											

Fig-3:Table 3 Matrix 3

2.3 Block Diagrams

Block diagrams of our proposed algorithm for encryption and decryption are given below.

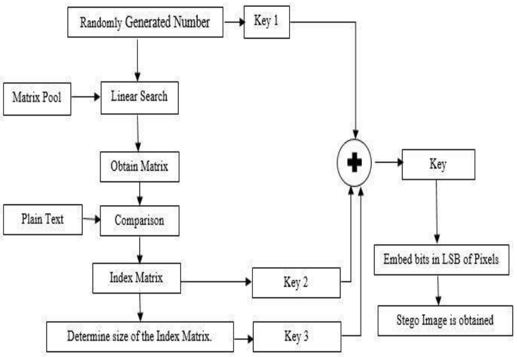


Fig-4:Encryption block

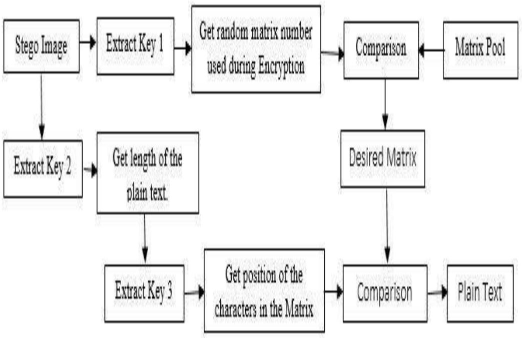

Stego Image
Extract Key 1
Get random matrix number used during Encryption
Comparison
Matrix Pool
Extract Key 2
Get length of the plain text.
Desired Matrix
Extract Key 3
Get position of the characters in the Matrix
Comparison
Plain Text

Fig-5:Decryption Block

2.4 Results and Analysis

Encrypting the message:

Plain text: “Attack at dawn” and the random matrix selected is

{	j	%	y	n	c	a	]	G	^	z	W	X	w	U
Y	F	+	t	L	P	s	7	9	f	h	#	,	6	u
1	m	O	x	}	>	|	l	'		Q	e	0	5	@
d	Z	?	3	p	[	k	g	$	:	J	E	/	4	R
-	b	o	=	V	A	v	K	;	I	<	q	_	H	~
!	r	M	2	B	(	\	8	.	*	C	D	)	i	&
"	T	S	N											

Fig-6:Table 4 Matrix 4

After encrypting the message key is automatically generated which in this case is 0010001110001010000100010011001001100001110000110011010001010000000111001001101010000101110000011100011100000101

2.5 Hiding the Key in the Image

The key so generated is then embedded in the LSB of the pixel values of the image and thus the message is concealed. Due to changes in only one bit in the pixel values the image does not distort much and the message is safely transmitted.

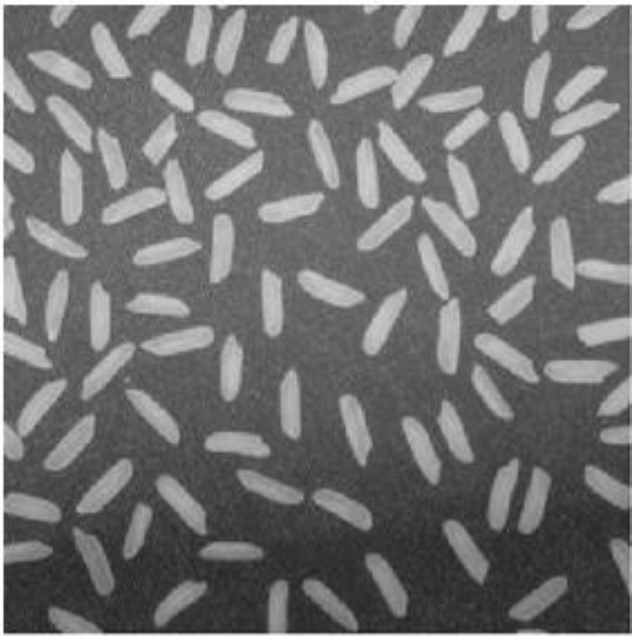


Fig-7:The original image

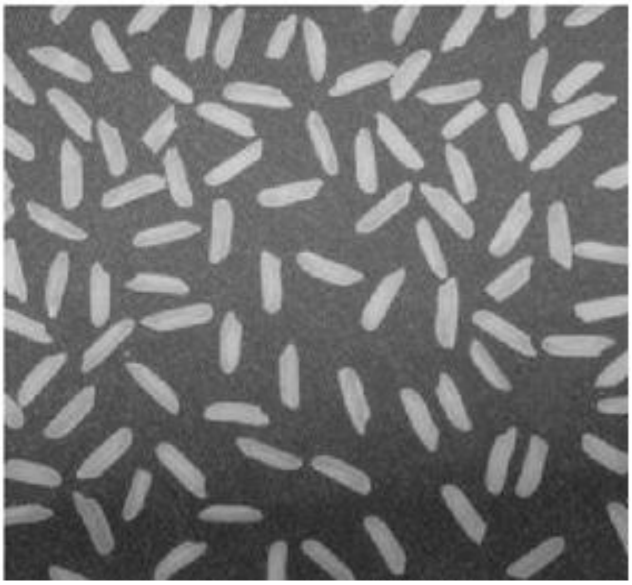


Fig-8: The image containing hidden key

The correlation between the two images results in a 99.98% match. And the signal to noise ratio between the two images gives a result of 83.2853 %.

The following two bar graphs show the variation of the pixel values in the image for the first 112 pixels which is the length of the key.

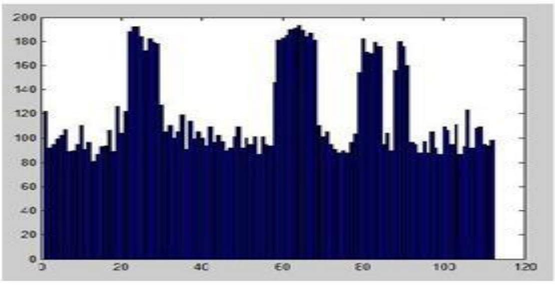


Fig-9: Bar graph showing the first 112 pixel values of the stego image.

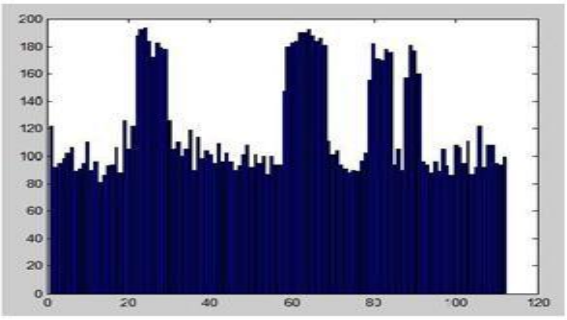


Fig-10: Bar graph showing the first 112 pixel values of the stego image

Thus it is seen from the graphs that the distortion in the image is very negligible resulting in a microscopic chance of detection the message.

3. CONCLUSION

Cryptography [8] and Steganography [3] are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Cryptography [8] is the study of securing information without hiding the means of communication. We cannot achieve cent percent security [4][5]. So bi-fold or hybrid systems started emerging. The method of obfuscation proposed in this algorithm provides three layers of security to the transmission of data. The first layer being the random number generator, the second being the matrix pool and the third is the LSB based Steganographic approach. As every user pair will have a unique set of matrix, the chances of detecting the information reduces significantly. This feature can be employed reliably on systems that require one to one communications.

4. REFERENCE

[1] William Stallings: ―Cryptography and Network Security: Principles and Practices 4th Edition, Prentice Hall.

[2] Seyed Rahman Soleimani, Masood Niazi Torshiz, ”A New High Quality Vision Non-Adaptive Steganographic Method, Using Module and Combined Functions”, International Journal of Emerging Trends in Signal Processing, Volume 1 ,Issue 2, January 2013

[3] A.Joseph Raphael, Dr.V Sundaram, ”Cryptography and Steganography - A Survey”, International Journal of Computer Technology and Applications, Volume 2 ,Issue 3, May 2011

[4] Dipta Mukherjee, Anandarup Mukherjee, Somen Nayak, “A Hybrid Stegano- Cryptographic Approach to Data Obfuscation Using LSB Technique”

[5] Moutushi Singh, Rupayan Das “Survey of Different techniques to Detect wormhole attack in wireless sensor Network” published in International Journal of Scientific & Engineering Research (IJSER), Volume 3, Issue 10, and October-2012 ISSN 2229-5518

[6] Rahul Sourav Singh,Rupayan Das, Dipta Mukherjee,Prannay Bothra , “RDR cube cipher an extension to Vignere Cipher”,IOSR Journal of Computer Engineering(IOSR-JCE) e-ISSN:2278-0661,p-ISSN:2278-8727 Volume 16,Issue 2,Ver.III(Mar-Apr.2014),PP 64-71

[7] Anindya Shankar Shukla,Rupayan Das,Rahul Sourav Singh,Dipta Mukherjee “Bar Cipher: A Robust technique for data hiding using the concept of Barcode”,Procedings of 1st International Science & Technology Congress 2014,Elsevier publication,ISBN: 9789351072485

[8] W. Bender D. Gruhl N. Morimoto A. Lu “Techniques for data hiding” IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4, 1996