RESEARCHERID
THOMSON REUTERS

[Sahana* 4(3): March, 2017] ISSN 2349-4506
Impact Factor: 2.785

Global Journal of Engineering Science and Research Management

MULTI-LAYERED RGB BASED SECURE TECHNIQUE FOR DATA TRANSFER

Jenifar Khan, Subham Sengupta, Sudipta Sahana*
Department of Computer Science & Engineering, JIS College of Engineering, Block–A, Phase–III, Kalyani, Nadia–741235, West Bengal, India
* Assistant Professor, Department of Computer Science & Engineering, JIS College of Engineering, Block–A, Phase–III, Kalyani, Nadia–741235, West Bengal, India

DOI: 10.5281/zenodo.439256

KEYWORDS: Induced Dynamic Table, Axis Rotation Table, Four Face Cube, RGB, Cipher.

ABSTRACT
Network Security has become very important in today's world, as a result of which various methods are adopted to bypass it. Network administrators need to keep up with the recent advancements in both the hardware and software fields to prevent their as well as the user's data. The paper briefly introduces the concept of data security i.e. a manually generated shift key based cryptographic technique which (de)ciphers the fragmented plain text. Here both encryption and decryption methodologies are proposed. The paperwork outlines a cryptographic algorithm based on a user defined shift key modus operandi engendering ciphers at bay. First, it creates an IDT (Induced Dynamic Table) to refer the position of the plain text characters. Then the next cipher is fabricated by setting the ART (Axis Rotation Table) according to the shift key. Subsequently, the further cipher is induced by a FFC (Four Face Cube). Later, the new partial cipher text characters are put into a definite sequence to get the standard color palette in RGB format. Hence, our final cipher with the shift key characters at the additional first and last color respectively in RGB format is generated. During decryption methodology, the color is selected and is opened in the standard color palette. The RGB values of the special characters has their own signature to what makes them different from the other plain characters in the time of decryption. The proposed methodology ensures significant use in both, data transfer and network security.

INTRODUCTION
During this time when the Internet provides essential communication between tens of millions people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords.

One essential ingredient for secure communication is that of Cryptography. The concept of securing messages through cryptography has a long history. Indeed, Julius Caesar is credited with creating one of the earliest cryptographic systems to send military messages to his generals.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to preserve sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. It's a method that allows information to be sent in a secure form in such a way that, only the receiver is able to retrieve this information. While cryptography is the science of securing data, cryptanalysis is the science of scrutinizing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

A cryptographic algorithm or cipher, is a mathematical function used in encryption and decryption process. The algorithm works in combination with a key to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all possible keys and all the protocols that make it work compromise a cryptosystem.

Now-a-days cryptography has many commercial applications. If we are protecting confidential information then cryptography provides high level of privacy to individuals and groups. However, the main purpose of cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like- data integrity, authentication and non-repudiation.

RELATED WORK

In Mathkour *et al* [1], a spiral-based Least Significant Bit (LSB) approach has been presented for hiding messages in images and the key idea is based on the LSB substitution technique applied on RGB color components of BMP images. The proposed idea is to divide the image into segments and process them differently.

In P.Marwaha et al. [2] the proposed Cryptography and steganography are the most widely used amidst modern techniques. Although these techniques provide some level of security of data but neither of them alone is secure enough for sharing information over an insecure communication channel and are vulnerable to attackers.

In Vivek et al. (2012) [3] a prominent method has been proposed to implement the steganography and cryptography for concealing the data into a medium. The steganography medium used in this data hiding system is audio and Least Significant Bit (LSB) algorithm is used for encoding the message in the cover medium.

In Raphael et al. (2011) [4] the engendered algorithm focuses on how combining both steganography and cryptography will provide better security and confidentiality.Cryptography makes the information incomprehensible. However, steganography put light on hiding the existence of the vital data.

Monalisa Dey et al. [5] presented an efficient and vital security actions to fortify data confidentiality. It only deals with binary data to cover all sorts of data in the field of Computer Science.Therefore,corrobating data security notwithstanding on what information is being traded..

In S.Sahana et. al [6] have contemplated an exclusive technique for encryption with a fixed user defined key and concealing the cipher text inside a gray scale image for utmost certainty.

In Diaa Salama Abdul. Elminaam et al. [7] assosiated a number of the encryption algorithms with heterogeneous settings for apiece algorithm such as distinct sizes of data blocks, distinct data types, diverse key sizes, battery power efficiency and the ultimate encryption/decryptionrate.

THE SCHEME

In this approach, an algorithm is defined that is much safer and secure then the rest as it goes into the multiple levels of encryption with giving flexibility to the user to choose the depth of security. Moreover, all the data values that appear in the final cipher text are unique in the data set. These data sets are in turn unique and different for any value or text in the universal space.

Step 1: At first, assuming an arbitrary Shift Key of two characters where the first character is a numeric digit and the second character is any uppercase alphabet (e.g. 4D).

With the help of the shift key, a proposed table is commenced (Induced Dynamic Table). In this table, the first element of the header row is the first shift key character and the second row first element is the second shift key character. Continue to pad the rows with the following alphabets and possible numerical digits respectively.

Now, each of the rows encodes one plain text character. The first row conceals the first plain text character, the second rows conceals the second pain text character and so on. So, the number of rows in IDT is equal to the number of alphanumeric characters in the plain text.

For each row, the cipher character will be the header row character in position. After the tabular conversion, we get our first cipher text with the special characters unchanged.

NOTE: While converting any uppercase plain character into first cipher, if any numeric digit has got as a cipher character, a backslash("\") is added before that cipher character and remains unchanged until the final cipher gets produced for its distinction. Then it gets converted with the algorithm for special characters.

Step 2: Next, with the implementation of the ART (Proposed circular table named Axis Rotation Table), our second cipher is accomplished In ART,there are axes for three different types of characters. X for uppercase alphabets, Y for lowercase alphabets and Z for numeric digits.
The axes are represented in a circular table form (for the convenience to understand), there are total ten sections in
the table.
Each section is divided as follows:
1. in four parts for X axis.
2. in three parts for Y axis.
3. No division for Z axis.

Setting the ART: The rows of the table or axes of ART are set according to the shift key. The first shift key character is adjusted in the Z axis and the second shift key character is placed in the X and Y axis. Subsequently, the ART is set for the further encryption.

In the next stride, for detecting the characters of first cipher text in ART, follow the rules underneath:

1.Look for the letter in the axis, if it is in the right half then 2 is recorded; or else 1 is taken for the left half. So, the first character is always either 1 or 2.
2. Look for the axis in which the character is present i.e. among X, Y or Z. So, the second character is either X, Y or Z.
3. Search for the location of the character in the axis. The position is calculated as the number of completed section and division number. So, the fourth character is the number of sections completed, and the third character is the division number.
Therefore, the second cipher text is developed by discovering where the character lands in ART. In which each consecutive four letters represent one character of first cipher text keeping the special character as it is.
Step 3: Next, FFC (Proposed Four Face Cube) is introduced in the generated cipher text. Each face has four segments.
Initially, the cipher text characters on the four faces of the Cube are plotted.
Accordingly, each four consecutive characters from second cipher text are allocated in the front face of the FFC by gyrating the segments of the cube. Consequently, the direction for each segment is listed. Furthermore picking the directions as vectors with equal magnitudes, we get the resultant vector.
It has been observed that eight possible resultant vectors can be obtained in the Cartesian coordinate here. Thus, the individual resultant lines are denoted with two numeric digits. First one, is for determination of half of the coordinate (i.e. 1 or 2) and second one is for the possible number they are in i.e. the angle.
So, total of eight numeric digits are retrieved from the initial cipher. One extra bit is added as the 9th character. If the position of the plain text character is odd then the extra character is 1 and 2 for even positions. Next these digits are planted in a sequence of "1 2 3 – 5 4 6 – 7 8 9" positions accordingly to get the value for RGB.

For Special Characters:
The ASCII value of special character and each distinct character of shift key are acquired to convert special character into a significant cipher.
Shift Key: 4D
RED = ASCII of first shift-key character + 80 –ASCII value
GREEN = ASCII of second shift-key character + 80 –ASCII value
BLUE = ASCII value + 80
Next the RED, GREEN and BLUE values are used to produce the color.

The Implementation

Encryption Methodology

Plain Text: "Hit"
Shift Key: 4D

Step 1:

Commencing the IDT with shift key "4D"-

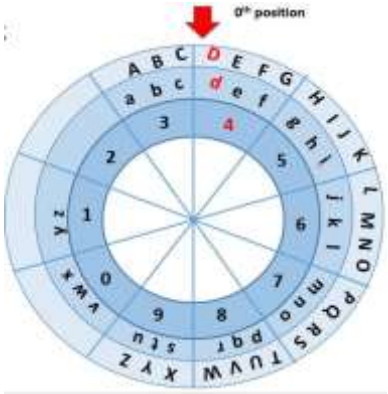
4	5	6	7	8	9	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E

Induced Dynamic Table

Starting the header row with first shift character and then starting the element rows with next Shift-key character, we get "\88i" as our first cipher text of "Hit" from IDT.

Step 2:

Next we set the ARA with the shift characters in 0th position-
The first cipher text is converted into second cipher text by adhering to the rules below-



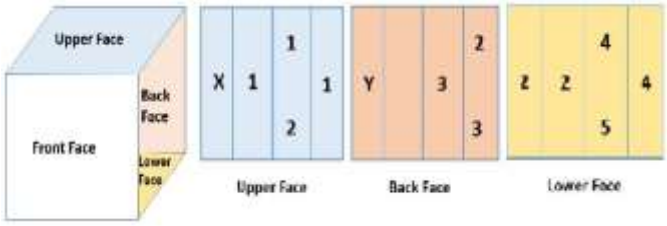
Axis Rotation Table

1st cipher	Axis	Direction 1 (Left) /2(Right)	No. of Complete Sections	No. of Divisions	2nd cipher
\	.	.	.	.	\
8	Z	2	5	1	Z251
8	Z	2	5	1	Z251
i	Y	2	2	3	Y223

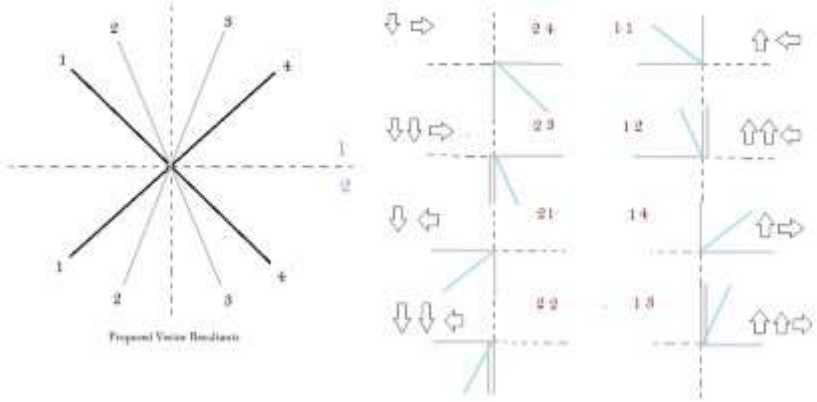
Hence the second cipher text is: " \ Z251 Z251 Y223 "

Step 3:

Afterwards, the final cipher text is consummated from the 2nd cipher text through FFC. Special characters are too converted into RGB format in this step.



Four Face Cube



Vector Resultants

Note: If the cubic rotation is downwards then there is a right-shifting, and for upwards rotation there is left-shifting. For the back face, characters shift according to their position. Character on the top shifts right and the bottom character shifts left after rotating the segment.

Third Cipher	Characters	Rotation	Shift	Denotation	Extra Character	Final Cipher
Z241	Z	Up	Left	11	1	111-114-141
	2	Up	Left	11		
	5	Up	Right	14		
	1	Down	Right	14		
Z241	Z	Up	Left	11	2	111-114-142
	2	Up	Left	11		
	5	Up	Right	14		
	1	Down	Right	14		
Y223	Y	UpUp /DownDown	Left/Right	12/23	1	231-121-131
	2	Up	Left	11		
	2	Down	Right	21		
	3	UpUp /DownDown	Right	13/23		

Note: User can use any of the final cipher values.
The highlighted final cipher values have been taken for the final color implementation.
Note that the produced cipher is again rearranged in 1 2 3 – 5 4 6 – 7 8 9 manner to get the color code.
This makes the cipher 111-114-141 111-114-142 231-211-131

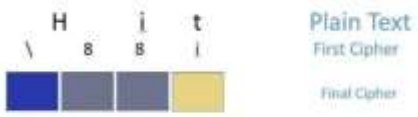
Algorithm for converting Special characters

Shift Key: 4D

Shift Key Character	Value	ASCII
Character 1	4	52
Character 2	D	68

Special Character: \
ASCII value of Special Character: 92
RED = 52 + 80 – 92 = 40
GREEN = 68 + 80 – 92 = 56
BLUE = 92 + 80 = 172
Next the RED, GREEN and BLUE values are used to produce the color.

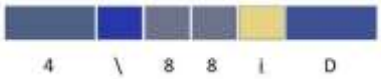
So, we get 040-056-172 as the RGB value for '\' character.
Hence the final cipher of the plain text "Hit" that has been produced with shift key "4D" is-
040-056-172 111-114-141 111-114-142 231-211-131.



Final Cipher String

Step 4:
Till now the shift key has not been incorporated in the final cipher. To add the shift key in the cipher, two additional colors are required. We use the same algorithm which converts the special characters to produce the two color in addition. The first color will be formed from the first character of the shift-key and it is added before the final color string as the first color. The second color is formed from the second shift-key character and is placed after the final color string as the last color. Using the algorithm we get the color as follow-
For the first character:
RED = 52 + 80 - 52 = 80
GREEN = 68 + 80 – 52 = 96
BLUE = 52 + 80 = 132
So the RGB value is 080-096-132 for the first shift-key character.
For the second character:
RED = 52 + 80 – 68 = 64
GREEN = 68 + 80 – 68 = 80
BLUE = 68 +80=148
So the RGB value is 064-080-148 for the second shift-key character

Hence, the final cipher including shift key is-
080-096-132040-056-172 111-114-141 111-114-142 231-211-131 064-080-148
Conversion of the final cipher into RGB color code:



Final Cipher String with embedded shift-key

This is the final cipher text included shift key in RGB format which is to be sent to the receiver.

Decryption Methodology
Extraction of the Shift-key

In the receiver end the first task is to extract the shift key from the color-string. Hence the RGB values of the first and last color is extracted.
From the color string we get 080-096-132 and 064-080-148 as the RGB values of the first and the last color.

Subtracting 80 from the BLUE value of both the color, we get the ASCII value of first and the second shift-key character respectively.
ASCII of first shift-key character = 132 – 80 = 52
ASCII of second shift-key character = 148 – 80 = 68
Commencing the procedure we get our shift-key as 4D.

Sorting out the Special Characters
As we have used one algorithm to encrypt the regular alphabets with digits and another algorithm to encrypt the special characters, the special characters are sorted from the alphabets and digits in order to use the different decryption algorithms. Note down that the RED value of any color that we get encrypting a special character, is always less than equal to 105. In the other side, while encrypting the regular alphabets and the digits, the RED value of any color cannot be less than 111. In this context we can say that the colors with RED value less than or equals to 105 are the encrypted form of any special character and the rest are either regular alphabets or digits. After sorting the encrypted color of the special characters out from the color string, for decryption we practice the reverse of the encryption algorithm that we used for the special characters.

Decrypting Alphabets and Digits
The cryptographic algorithm is subsequently followed in reverse order for alphabets and digits.
Hence, the plain text is engendered.

RESULTS AND DISCUSSION

In our algorithm we have given RGB based color form to the plain text in order to commence the encryption. We have used different algorithm to encrypt the special characters along with the alphabets and digits. The algorithm is based on using a two digit random shift key which provides pseudo-randomness in the algorithm. The encryption process is divided into more than one layer hence which makes it more complex to decrypt. The final RGB form can be used in steganography and chromatography in future aspects. From the following result analysis it is clear that the process consumes almost same time whether it is trying to encrypt a small or rich content file.

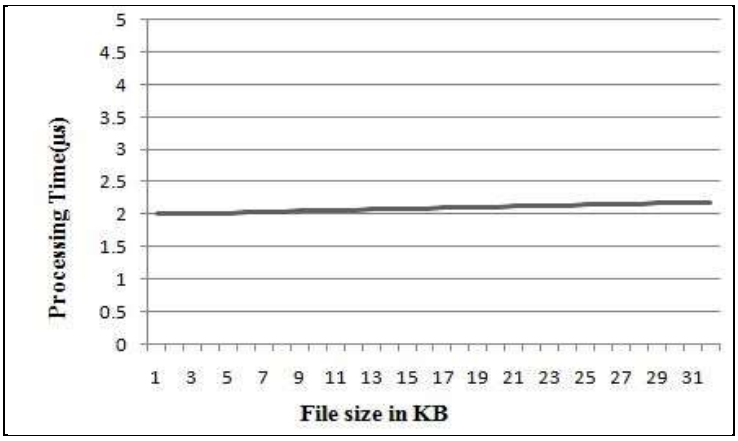


Fig. 1 – File Size vs. Time

CONCLUSION

From the result it is clear that our 'proposed algorithm' is better due to the key updating concept i.e. a new approach to increase the difficulty to discover the key. It has been found that the algorithms which are available at this moment are easy to decrypt using some pattern more or less complex in nature. Because those algorithms

are used to maintain high level of security against any kind of forgeries. For a very minimal amount of data those algorithms wouldn't be cost effective since those are designed for small amount of data. The aim of this work was to design and implement a multi layered algorithm to address this issue. The same can be extended to texts and large data values. Keeping this goal in mind the proposed algorithm has been designed in quite simpler manner but of course not ablating the security affairs.

The important thing of our proposed method is that it is almost impossible to break the encryption algorithm without knowing the exact key value. We proposed that encryption method can be applied for data encryption and decryption in any type of public application for sending confidential data. So, it provides useful applications in the field of network security.

ACKNOWLEDGEMENTS

We are grateful to Department of Computer Science and Engineering, JIS College of Engineering for providing the lab facility towards conducting the research work.

REFERENCES

1. A Novel Approach for Hiding Messages in Images by Mathkour, H. ; Assassa, G.M.R. ; Al Muharib, A. ; Kiady, I. Signal Acquisition and Processing, 2009. ICSAP 2009
2. Piyush Marwaha, Paresh Marwaha, "Visual Cryptographic Steganography in images", 2nd International conference on Computing, Communication and Networking Technologies, 2010
3. Vivek, J., Lokesh, K., Madhur, M. S., Mohd, S., and KshitizRastogi 2012. Public-Key Steganography Based on Modified LSB Method. Journal of Global Research in Computer Science, 3(4). ISSN: 2229-371X, pp. 26-29.
4. Raphael, A. J., and Sundaram, V. 2011. Cryptography and Steganography - A Survey. International Journal of Computer Technology Application, 2(3), ISSN: 2229-6093, pp. 626-630.
5. MonalisaDey, Dhirendra Prasad Yadav, Sanik Kumar Mahata, AnupamMondal, Sudipta Sahana, "An Improved Approach of Cryptography using Triangulation and MSB Iteration Technique"Special Issue of International Journal of Computer Applications (0975 – 8887) International Conference on Computing, Communication and Sensor Network (CCSN) 2012
6. Sudipta Sahana, Abhipsa kundu, Ahana Pal, "Crypt arithmetic stego based encryption algorithm" in International Journal of Computer Applications.(ISBN-973-93-80879-46-7) Nov 2013
7. Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.