A NEW COLOR ORIENTED CRYPTOGRAPHIC ALGORITHM BASED ON UNICODE AND RGB COLOR MODEL

Panchami.V[1], Varghese Paul[2], Amithab Wahi[3]

[1]*Asst.Professor, Computer Science & Engineering, TocH Institute of Science and Technology, Kerala, India*
[2]*Professor, Department of Information Technology, CUSAT, Kerala, India*
[3]*Professor, Department of Information Technology, Bannari Amman Institute of Technology, Tamil Nadu, India*

Abstract

RGB color oriented cryptography is a new research area in data security. In this paper a new approach to encrypt and decrypt information independent of the language using colors is proposed. The message of any language consists of set of Characters, Symbols, and Digits, and is encoded using UNICODE, so that any language can be encrypted. The UNICODE value of each character in the message is encrypted using the RGB color encryption method and is then compressed. Each cipher color has an equivalent hexadecimal value. This hexadecimal values is converted into its binary equivalent form. The binary values thus obtained are divided into two equal parts. The first part is treated as message and the second part is treated as key. XOR operation is applied between the two parts and thus achieving compression. In order to secure the key is encrypted using the RSA encryption algorithm. The last step of this proposed algorithm is optional, the cipher message is again encrypted to cipher color and then send through the insecure channel. If we want to hide the color information avoid this last step.

Keywords: *UNICODE Encoding, RGB color model, Data Compression.*

----------***----------

1. INTRODUCTION

The concept of using RGB color in cryptography has been identified as an innovative technology for constructing powerful unbreakable algorithms. To design a secure and strong encryption method for Multilanguage messages is very hectic and tedious task, for developing such type of algorithm involves complex problems to achieve higher degree of security. UNICODE [3] is a computing industry standard for the consistent representation and handling of text expressed in most of the world's writing systems. Developed[5][9] in conjunction with the Universal character Set standard and published in book form as The UNICODE Standard[4][9], the latest version of UNICODE consists of a repertoire of more than 107,000 characters[5] covering 90 scripts, a set of code charts for visual reference[5], an encoding methodology[11] and set of standard character encodings, an enumeration of character properties such as upper and lower case, a set of reference data computer files[5], and a number of related items[9]. This paper introduces a new technique for cryptography by using the concept of DNA computing in collaboration with UNICODE and colors in universe. We can see about 1000 levels[4][5] of light and dark, 100 levels of red and green, and 100 levels of yellow and blue for a single viewing condition in a laboratory[3][9]. This means that the total number of colors we can see is 10 million colors [5][6]. A computer can display about 16.8 million colors [9] to create full color pictures[9], really more than necessary for most of situations[3][4]. The appearance of a color is greatly affected by the viewing conditions, which include the color of the lighting, the amount of lighting [9], and other colors in the scene. Colors also appear in different modes [9] when they appear on different objects such as surfaces, light sources, or within volumes [4][5][7]. Since we can see at least 10-million colors [4][5] in a single viewing condition and the variety of viewing conditions and observers is endless[9], then the only truly correct answer is infinity. If we have 10-million colors[3][5], times 10-million lighting types, times 10-million lighting levels, 10-million surrounding colors, times 6-billion people in the world, using these modes of viewing we get a really huge number[4][5]. Each color is unique and can be represented in hexadecimal values [4], so we can represent any data or user in colors, this is the advantage that we see while using colors [3] in our encryption and decryption algorithm [3]. The best way of achieving [3][9] a robust system is to act on scalability that is to reach a large scale complexity for the problem. As some of the modern encryption algorithms are broken, there arises the need for some new directions of information security. This paper proposes a RGB based data encryption algorithm to secure the data communication. This paper is organized as follows: Section 2 describes the proposed algorithm for encryption. Section 3 illustrates the encryption method with example. Decryption mechanism is explained in section 4 and section 5 deals with conclusion and future enhancements.

2. PROPOSED SYSTEM

The plain text is encoded using UNICODE then it is encrypted using the RGB colour model [4][9]. Compress the color using color compression technique. Convert the color into binary streams, divide the binary stream into two equal part then apply XOR operation to achieve compression again. Half part of the cipher message is treated as the key. Key exchange is done using RSA [5][6] algorithm. Last part is optional the cipher text is again converted to colors and sends.

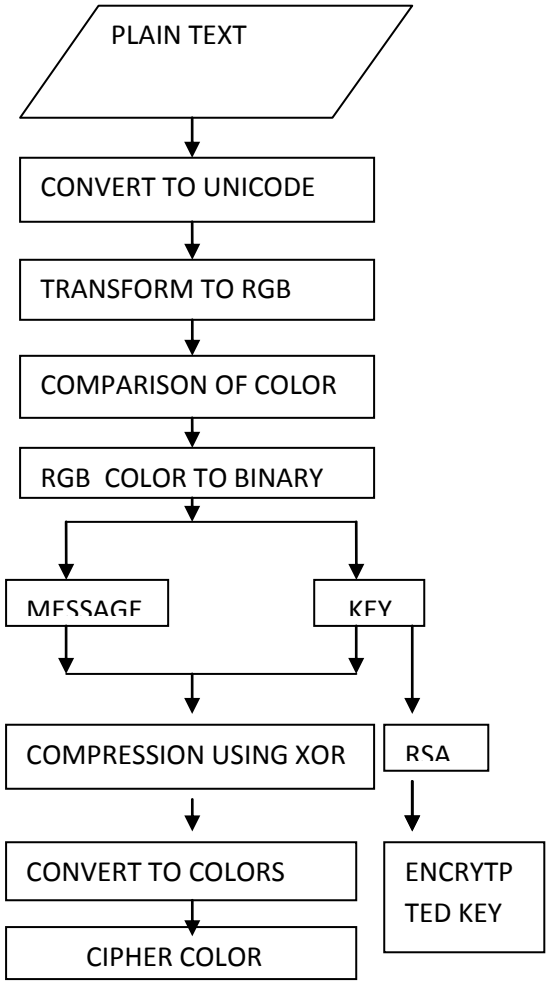


Fig -1: Flow chart of the Color Based algorithm

3. ENCRYPTION

The plain text is encoded using UNICODE then it is encrypted using the RGB colour model [4][9]. Compress the color using color color compression technique. Convert the color into binary streams, divide the binary stream into two equal part then apply XOR operation to achieve compression again. Half part of the cipher message is treated as the key. Key exchange is done using RSA [5][6] algorithm. Last part is optional the cipher text is again converted to colors and sends.

3.1 Encode Plaintext Using UNIDODE

The characters, symbols, digits of any language are encoded using UNICODE [5][7]. The objective of UNICODE is to unify all the different encoding schemes so that confusion between computers can be limited as much as possible. The advantage of UNICODE [4] compared to ASCII is that it can encode characters from multilingual plane. ASCII can encode characters only from English language [3][5]. These days the UNICODE standard [4][5] defines values for over one million characters and can be seen at the UNICODE Consortium[5]. It has several character encoding forms [5], UTF standing for UNICODE Transformation Unit.UTF-8[4] only uses one byte (8 bits) to encode English characters[5]. It can use a sequence of bytes to encode the other characters[5]. UTF-8[5] is widely used in email systems and on the Internet. UTF-16 uses two bytes (16 bits) to encode the most commonly used characters [3][5]. If needed, the additional characters can be represented by a pair of 16-bit numbers. UTF-32[4] uses four bytes (32 bits) to encode the characters[5]. It became apparent that as the UNICODE standard grew a 16-bit number is too small to represent all the characters [5]. UTF-32 is capable of representing every UNICODE [4][3][5] character as one number. In this proposed algorithm, we are using UTF-16 for encoding the plain text to UNICODE values. In this proposed new policy, first of all it checks each and every character in the given file. Then it finds what equivalent UNIODE of each character is.

3.2 Encrypt Using RGB Color Model

The characters in the plain text are translated into colors. After encoding, each and every characters, symbols, digits of any language are encrypted into colored-charts [3][5]. The UNICODE [4] of each character is converted into colors using following Table 1, which provides a mapping of UNICODE and colors. A computer displays about 16.8 million colors [5] to create full color pictures, really more than necessary for most situations[9]. Now we are considering 10 million Colors only. And the UNICODE standard [5] defines values for over 100,000 characters[5] and can be seen at the UNICODE Consortium. Now 10 million colors and 100,000 characters are available in a computer system [5][6]. Now we can create a dynamic mapping table. As we said earlier, computer screen supports millions of colors[5][3], so we can create millions of dynamic color-chart tables. In each table [4] there are four columns unique id, the data, the Unicode of that data and the color. Each table is identified by unique id number, that unique id number acts as first private key (KEY 1) while decrypting the message. This provides more difficulty in decryption side. According to the Table 1, an example is as follows:

Table -1: Colored Chart Table

Unique ID for each color	Character(any language) / Symbols /digits	UNICODE	Colors
1	A	U+0041	
2	B	U+0042	
3	C	U+0043	
4	D	U+0044	
5	E	U+0045	
. .	. .	. .	. .
25	1	U+0031	
26	2	U+0032	
. .	. .	. .	. .
33	#	U+0023	
34	Space	U+0020	

Consider the character "A". The UNICODE of "A" is U+0041.This UNICODE is converted into the equivalent color which is black. Similarly "B" is U+0042 which is blue, "D" is U+0044 which is green, "E" is U+0045 which is yellow. The following Figure 2 shows color code equivalent of the word 'BADE'.

After RGB color Encryption:

Fig- 2: Color code equivalent to the word BEAD

We will also check if the two adjacent colors is same or not, that means if the plain text have adjacent same characters, then we will replace it with another color as in the given table, (Table 2). For each time the adjacent color arrives it is replaced with each unique color as in Table 2, the time is taken as second private key (KEY 2).The aim of this step is to achieve compression, and can reduce the size of the encrypted data. This compression technique is very simple as well as it's very efficient and effective for any type of data.

Table -2: Colored chart table

No. of times same color appears continuously	Color
1	
. .	
n	

3.3 Compression of Colors

The number of colors in the resulting set after the first step will be same as the number of characters in the plain text.

For a huge amount of data we will get a combination of a lot of colors for which the maintenance task is complicated one and not efficient. So we go for compression by mixing adjacent two colors. Each color has its own unique hexadecimal value [7]. If we mix two colors we will get another color which has a unique hexadecimal value, which means the resultant color can be produced only by mixing with those two colors. Each color has its own unique ID. This unique ID is used at the time of decryption to retrieve the component colors [6]. This set of unique IDs is treated as the third key, KEY3. So we input the hexadecimal value of the resultant color to a color blending tool, it will give those two colors with their hexadecimal values. Generation of keys: KEY 1, KEY 2, KEY 3. The three keys are sent to the receiver using key agreement proposed by Diffie-Hellman [2]. From the above example, mixing of two adjacent colors is shown in figure 3.

Fig 3: Compression of colors

Fig 4: Result after 1st stage of compression

3.4 Conversion of Colors to Binary Form

Every color in RGB model has an equivalent hexadecimal code [7]. Color codes are hexadecimal triplets representing the colors red, green and blue (#RRGGBB). For example, for red color, code is #FF0000, which is '255' red, '0' green and '0' blue. See Figure 5.

Fig -5: Colors and their hexadecimal values

For further proceeding, we need to convert this hexadecimal code to a binary equivalent form. Now the hexadecimal code of the final color is considered and this code is converted to the binary form through simple hex to binary conversion. Now, the binary value we obtained is divided and treated as two parts-1.The message 2.The key

3.5 Compression of Data

The message and key that we obtained in binary format is again compressed by performing simple XOR operation on bits [8]. So that we can reduce the size of encrypted message .Since the compression using XOR is being performed, we can easily extract the message and key later by using reverse XOR operation. The key is now encrypted using RSA [9].

3.6 Conversion of Cipher Text to Cipher Color

As the final step, the cipher text is encoded as colors by referring to the Figure 1. Last part is optional the cipher texts is again converted to colors and then send through the insecure channel. If we want to hide the color information avoid this last step.

4. ILLUSTRATION WITH EXAMPLE

In this example the Plain Text is BEAD.

4.1 Unicode of Each Character

- B - U+0042
- E - U+0045
- A - U+0041
- D - U+0044

4.2 Conversion to RGB Colors

According to the Fig 2, the UNICODE of each character in the 'BEAD' is encoded to RGB colors as follows:

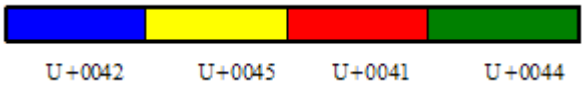


Fig -6: UNICODE is encoded to RGB Colors

4.3 Compression of Colors

Adjacent two colors are mixed to achieve compression. Blue and yellow is mixed to get ash color, red and green is mixed to get yellow.

Fig -7: Result after the compression

4.4 Compression of Colors

Fig -8: Result after the compression

These hexadecimal values of each color are converted into binary values.

#808080 : 100000001000000010000000
#FFFF00 : 111111111111111100000000

Hence, the binary equivalent form of our plain text 'BEAD' is:

100000001000000010000000111111111111111110000000

This binary value is then compressed.

4.5 Compression of Data

The binary form of the plain text is now divided into 2 parts. They are the message and the key

Message : 100000001000000010000000
Key : FFFF00

The key value obtained is encrypted using RSA [9] algorithm and sent to the recipient. The compressed form using XOR is given below:

011111110111111110000000

This binary value act as the input is encrypted using DNA concept.

4.6 Convert to Cipher Color

After XOR operation the binary value is divided into 8 bits, convert the 8 bits into cipher characters. According to the Table-1 the cipher characters are converted into cipher color. This step is optional because the cipher text along gives much security, we can avoid the color encoding technique is used in our algorithm from the opponent. The three plaintext characters are replaced one color thus achieving compression through this step.

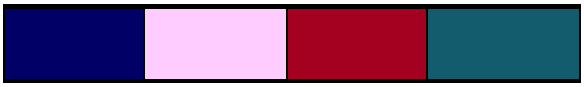
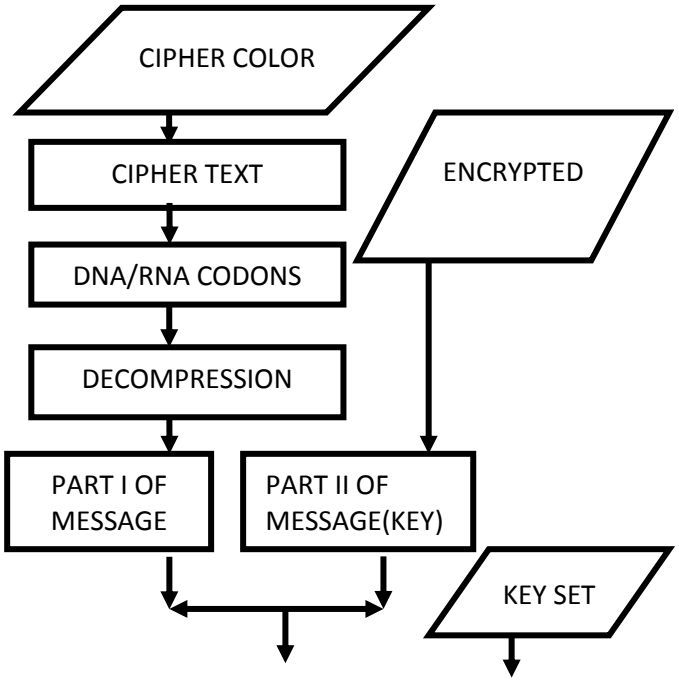


Fig -9: The Cipher Colors

5. DECRYPTION

The decryption process is simply the inverse of the encryption process. Here, we use a key set which consists of three keys. They are KEY1, KEY2 and KEY3. These keys are exchanged using Elliptic curve based Diffie-Helman[2] key exchange algorithm. In addition to the key set, we use another key which is encrypted by RSA [9] algorithm. In the proposed system key exchange is done using public cryptographic system.



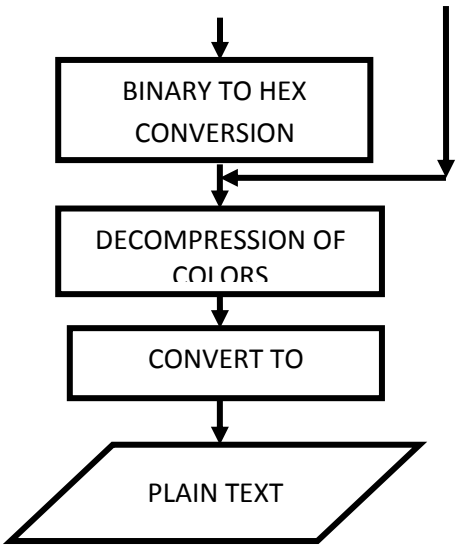


Fig-10: Flow chart of the proposed decryption algorithm

6. CONCLUSIONS

The proposed algorithm offers multilayer security. This technique is to open the door for the idea of applying the concepts of UNICODE, DNA and Amino Acids and colors to other conventional cryptographic algorithms to enhance their security features. We are using UNICODE so that we encrypt thousands of characters, symbols, digits etc of any language instead of the ASCII code. Then we are encoding with RGB colors. The advantage is that the display screen supports millions and millions of colors. Each color is unique. In the proposed algorithm, we are mixing the adjacent two colors. We can reduce the length to the half of the length of original message. If we are able to combine a group of colors and form a single color, we can represent messages of any length using just one color. So we can compress huge amount of data. In future we are planning to implement this encoding scheme on other known algorithms and measuring its performance and security. Experiments should be conducted to implement the algorithm on different applications to ensure its feasibility and applicability.

ACKNOWLEDGEMENTS

I sincerely thankful to my guide Dr.Varhese Paul and my joint supervisor Dr.Amithab Wahi for the continuous suggestions and feedback. I am very great full to Mr.Sudhin Vamattam, the Director of Aucupa Innovative solutions for his support in my research activities.

REFERENCES

[1]. " For number of color in the world" www.jimloy.com
[2]. "For number of color in the world" www.whyiscolor.org
[3]. Panchami.V," A Multilevel Security Scheme Based On UNICODE and RGB Color Model Using DNA Cryptography" IJCA Proceedings on Emerging Technology

Trends on Advanced Engineering Research - 2012 ICETT(3):29-34, January 2012. Published by Foundation of Computer Science, New York, USA. BibTeX
[4]. Suryavanshi H., Dr. Bansal P., Conference Proceedings of Ninth IEEE and IFIP International Conference On Wirless and Optical Communication Networks, IEEE ISBN: 9781467319881,IEEE DOI: 10.1109/WOCN.2012.6335543, 2012.
[5]. Maram Balajee "UNICODE and Colors Integration tool for Encryption and Decryption "published in International Journal on Computer Science and Engineering (IJCSE). ISSN: 0975-3397 Vol. 3 No. 3 Mar 2011
[6]. TAYLOR Clelland Catherine, Vivjana Risca, Carter Bancroft, 1999, "Hiding Messages in DNA microdots", Nature Magazine, Vol 399, June10, 1999.
[7]. Dominik Heider and Angelika Bamekow, "DNA-based watermarks using the DNA-Crypt algorithm", Published: 29 May 2007 BMC.
[8]. Piyush Marwaha and Parsh Marwaha, "Visual cryptographic steganography in images", Second International Conference on Computing, Communication and Networking Technologies,2010.
[9]. www.cis.rit.edu/fairchild/.../4-4.htmlReference 3
[10]. S.Pavithra Deepa, S.Kannimuthu, V.Keerthika, "Security using colors and Armstrong numbers', Innovations in Emerging Technology (NCOIET), Feb2011.
[11]. www.princeton.edu/~achaney/.../Unicode.html
[12]. S. Udaya Kumar, A.Vinaya Babu, 2006, "A Block Cipher using Color Substitution. IAENG Int. J. Computer. Sci., 32: 395-401.

BIOGRAPHIES

Panchami.V is a Research scholar in Anna University, Chennai. Now working as Asst.Professor in CSE department in TIST. She have 5 years of teaching experience. She is a B Tech. degree holder in IT and M Tech from Govt College Of Engineering, Salem in CSE. She has presented technical papers in many national and international seminars and conferences. She developed an Android application "ifollow"for ladies safety and got NASSCOM award for that app.

Dr. Varghese Paul has got more than 30 years of professional experience - in industry, utilities and academic institutions. Currently he is working as Professor in IT Department CUSAT. He was Dean (CS IT / Research), TIST. He acted as Head of Information Technology in CUSAT, SCADA Engineer in Electricity Department in Kingdom of Saudi Arabia, Communication Engineer in KSEB and Industrial Engineer in OEN India Ltd. Kochi. He is a B Tech. degree holder in Electrical Engineering, M Tech. in Electronics and Ph D. in Computer Science. He is a Certified Software Test Manager, Ministry of IT, Govt. of India. He had developed a special type of coding system, TDMRC Code and has many research publications to his credit and presented technical papers in many national and international seminars.

Dr.Amithab Wahi is working as Professor in IT department of Bannari Amman Institute of Technology, Tamil Nadu. He have more than 15 years in academics. His area of specialization are Image and video processing, Pattern Recognition. He is BSc degree holder in Physics, MSc in Solid state Physics and Ph D. in Neural Networks, Fuzzy Logic and Pattern Recognition .He have undertaken many Funded projects and has many research publications to his credit and presented technical papers in many national and international seminars.