Volume 3, Issue 6, June 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Performance Analysis of Color Based Cryptographic Algorithms

Hemant Suryavanshi [1]*, Dr. Pratosh Bansal

Department Of Information Technology,

Institute of Engineering and Technology, Davv, Indore, India

Abstract— The leading factors that influence any cryptographic algorithm are its ability to secure data and the speed and time efficiency with which it can secure the data. A timing evaluation model is generated and discussed in this paper to simulate the results and compare the performance of color based cryptographic algorithms. This paper considers three color-based cryptographic algorithms: UNICODE and Colors Integration tool for Encryption and Decryption, A Block Cipher Generation Using Color Substitution and An Improved Cryptographic Algorithm Using UNICODE and Universal Colors. The evaluation model considers same data to be processed by these algorithms and compare them based on the time each algorithm takes to perform the process of encryption and decryption. The results are simulated over files of different size to ensure the consistency of the algorithms. The evaluation model has been developed in C# language.

Keywords: Unicode, Public Key, Private Key, Encryption, Decryption.

I. Introduction

Cryptography came into existence thousands of years ago and till date has a vital significance in the field of data communication and information security. Information security simply means that information should be accessible only to the legitimate parties. For this purpose, cryptographic algorithms can be used. There are two broad categories of cryptographic algorithm namely public key and private key cryptography. Private key encryption is also known as symmetric key encryption. This type of encryption require that all the parties involved in communication must share the same key. This is the most common type of encryption used to encrypt large amount of data. Private key encryption is fast to process and easy to implement. Public key encryption, also known as asymmetric key encyption uses two dissimilar but mathematically related keys for encryption and decryption. A private and a public key pair is used for encryption and decryption. Plain text message encrypted with public key can be decrypted only with the private key and vice-versa [1]. The concept of public key cryptography is complicated as compared to private key. Public key encryption is more secure compared to private key encryption but is applicable to small amount of data due to its complex operations. A number of cryptography algorithms have been proposed so far for ensuring secure transmission of data, however due to the efforts of cryptanalyst they have been rendered useless overtime. The growth of internet and rapidly increasing E-commerce usage in day to day life motivates cryptographers to devise more secure solutions that ensures required data security. These security solutions are often subjected to security threats and cryptanlysis attacks, thus the solutions must be very secure such that they may not be easily deciphered.

II. Color Based Crptographic Algorithms

In this section a study of color based cryptography algorithms and the approaches followed by them is performed. The significance of colors in a cryptography algorithm is due to two main reasons: the wide range they offer for exploiting human visual system and the frequent use of multimedia data over the internet, this has led to the evolution of new technique of cryptography referred to as the visual cryptography. However visual cryptography is not discussed at length further in this paper.

In this section three color based cryptography algorithms are discussed:

- *UNICODE and Colors Integration tool for Encryption and Decryption****(Algorithm1)***
- *A Block Cipher Generation Using Color Substitution****(Algorithm2)***
- *An Improved Cryptographic Algorithm Using UNICODE and Universal Colors****(Algorithm3/Proposed algorithm)***

A. UNICODE and Colors Integration tool for Encryption and Decryption

"UNICODE and Colors Integration tool for Encryption and Decryption" [2] proposed by M. Balajee is a symmetric key algorithm based on Unicode encoding scheme and Universal colors supported by computer. The approach is to replace the plain text characters by colors. A range of colors is decided for a set of characters and accordingly a mapping table is maintained at each end prior to encryption/decryption. The private key is used to decide the range of colors. Here the author has utilized the large range of colors to perform encryption/decryption. The algorithm has employed the concept of confusion.

B. A Block Cipher Generation Using Color Substitution

"A Block Cipher Generation Using Color Substitution" [3] proposed by Lt. Ravindra Babu Kallam, Dr. S.Udaya Kumar and Dr. M. Thirupathi Reddy is a asymmetric key algorithm that works on a private and a public key. The approach here is similar to one proposed by M. Balajee but with extended features like authentication and confidentiality. This is also a substitution based algorithm that support the concept of confusion. ARGB color model is used for assigning colors. RSA algorithm is used to exchange the keys. The methodology used to convert the plain text characters to color based cipher text is discussed below:

Methodology Used:

- Select Starting address K1 and K1< N

Where: N =256X256X256X256 = 4, 29, 49, 67, 296,) (ARGB)

- Select Increment value K2 such that (K1 + (C X K2)) < N,

Where: K1 - Session key 1, K2 - Session key 2, C – Number of characters in the plain text, N- Maximum Number of colors

- Use RSA [4] Public key encryption algorithm for key distribution:
- Encrypt K1 and K2 using receivers (User B) Public key (PUB) for confidentiality
- Encrypt the result of step1 using senders (User A) Private Key (PRA) for Authentication.
- Send the result of step2 to the receiver
- Decrypt the result of step2 by using PUA
- Decrypt the result of step4 by using PRB

The approach used here makes use of RSA algorithm for key exchange. It is based on the concept of asymmetric cryptography where a public-private key pair is used. The algorithm uses ARGB color encoding for utilizing large range of colors.

C. An Improved Cryptographic Algorithm Using UNICODE and Universal Colors

"An Improved Cryptographic Algorithm Using UNICODE and Universal Colors" [4][5] is a symmetric key cryptographic algorithm which works on a single key for encryption and decryption. The mapping table used in the algorithm reduces the processing time and the mixing process enhances the security of data/information. The algorithm uses ARGB color encoding and Unicode character encoding. The methodology is discussed below:

Methodology Used:

Step 1: Enter the Key K. such that K is an numeric value
Step 2: Generate Color Mapping Table from This Key.
Step 3: Select The File Which you want to Encrypt
Step 4: For each character in the file do the following
{

a) Search the character in the color mapping database

b) Convert the ARGB value of That color in Binary Form

c) Reverse the value obtain in above step

d) Perform 3 bit Left Circular Shift to the value obtain in above step

e) Divide in to two part

f) Perform 3 bit Left Circular Shift to the first part

g) Perform 4 bit Right Circular Shift to the second part

h) Concatenate the two part

i) Generate the ASCII Value for Above Concatenated part

j) Create Dynamic Label and assign each label a ASCII Value
}
End For

The algorithm is based on substitution and transposition. In the first level the original plain text characters of the message are

replaced by the color values and in level second the color values are transformed to binary values, where mixing process takes place. The mixing process transforms the binary string generated to a random value which is read as the cipher text. This approach makes the algorithm more secure.

III. SIMULATION SETUP

The analysis tool for comparing the performance of color cryptographic algorithms is implemented in C#.net programming language.

C#.Net was chosen to implement the algorithm. The reasons for considering C# as the suitable technology for implementation are mentioned below [5][6].

- The language has a rich set of classes that can extend services provided by the CryptoAPI.
- Configuring and implementing the cryptography algorithm is easier in Net framework as it uses the omnipresent XML based configurations of algorithms.

A. Simulation Results

In order to evaluate the performance of cryptographic algorithms the following parameters were considered:

- Security
- Efficiency
- Bandwidth requirement
- Transmission time
- Encryption/Decryption time

✓ **Security:**

In the algorithms 1 & 2, the plaintext characters are converted color structure and are transmitted over the network. From a common perspective this seems to be secure approach as the ranges of colors used in the algorithms are very vast but from a cryptanalyst perspective this can easily be compromised by simple traffic analysis. The algorithms render a clue to the cryptanalyst that the original text is being replaced by a color value. Moreover it also provides a clue about the behavior of the algorithm. In contrast to these algorithms, the algorithm 3 has an additional level of security. With the algorithm, the plaintext characters are first converted to a color structure and then the color value is converted to an encrypted value. The two levels of encryption used over here ensure the security of the algorithm thus making it a better choice compared to the opponent algorithms.

✓ **Efficiency:**

The performance of the algorithm is highly affected by the operations incorporated in designing it. The algorithm 3 has simple circular shift operations. It does not involve multiple loops or conditional statements which are the major cause of poor efficiency. The simple operations used in the algorithm design make it work operate faster and hence create a scope for it to be used on different platforms by a variety of applications.

✓ **Bandwidth Requirement:**

The algorithms 1 & 2 are transferring data over the network in form of color structure which requires more bandwidth as compared to the text based algorithm. In the algorithm 3 the characters are converted to encrypted text values thus the algorithm has less bandwidth requirement which make it execute faster over the network.

✓ **Transmission time:**

The algorithms 1 & 2 convert the plaintext characters to 32 bit ARGB structure that increase the size of cipher text compared to the plain text, thus the transmission time is increased to a great extent. On the other hand, the algorithm 3 converts the plain text characters into text based cipher text characters thus ensuring the size of cipher text never exceeds the plaintext size and in turn the transmission time is lesser compared to the existing algorithms.

✓ **Encryption/Decryption time:**

The encryption /decryption time of algorithms have been evaluated on files of different size and varying contents. The table below shows the result:

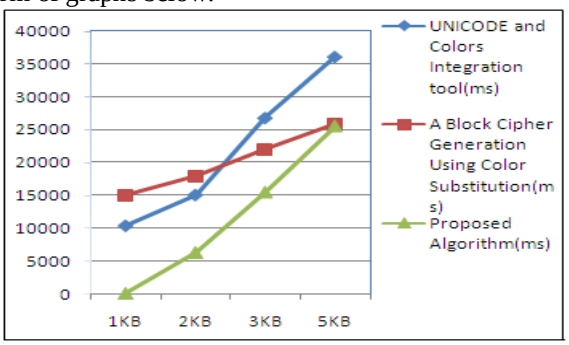
Table1: Encryption time for algorithms (in ms)

S. NO	File Size in KB	Algorithm 1	Algorithm2	Algorithm 3
1	1KB	10360	15063	94
2	2KB	15063	17875	6297
3	3KB	26797	22000	15469
4	5KB	36125	25859	25531

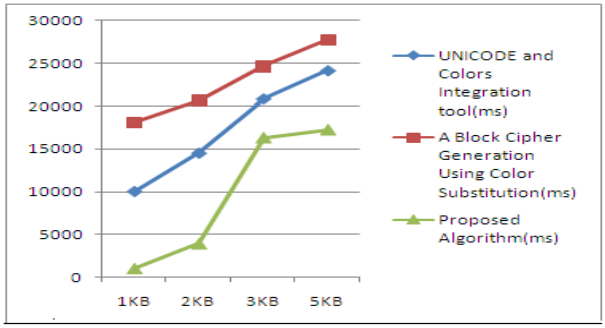
Table2: Decryption time for algorithms (in ms)

S. NO	File Size in KB	Algorithm 1	Algorithm2	Algorithm 3
1	1KB	10094	18078	1062.5
2	2KB	14563	20656	3938
3	3KB	20906	24656	16297
4	5KB	24187	27766	17234

Table1 & Table2 clearly shows that the time taken by the algorithm 3 is less compared to time taken by algorithms 1 & 2. The results are also represented in form of graphs below:



Graph1: Representing Encryption time of algorithms (in ms)



Graph2: Representing Decryption time of algorithms (in ms)

IV. Conclusion

The performance analysis of different algorithms has been performed to evaluate the results. It is observed that out of the three algorithms under consideration, "An Improved Cryptographic Algorithm Using UNICODE and Universal Colors" was found more efficient in context of security of information and time consumed for encryption/decryption process. "A Block Cipher Generation Using Color Substitution" among the three is an asymmetric algorithm that use RSA algorithm for secure key exchange, however the keys are exchanged securely but the algorithm used for encryption does not generate a very strong cipher text and the algorithm merely relies on substitution of characters into colors, the color based encryption may render clue to the cryptanalyst about the algorithm being used. "UNICODE and Colors Integration tool for Encryption and Decryption" is based on the simple approach of color based substitution replacing characters with colors. This algorithm also suffers from same demerit of rendering clue to the attacker. Moreover unlike ,"A Block Cipher Generation Using Color Substitution", it does not have any provision to exchange the keys securely. These serve as the major limitations of the algorithm. "An Improved Cryptographic Algorithm Using UNICODE and Universal Colors" is also based on color based substitution but it does not merely rely on the substitution, it further performs transposition on the binary value of color and transforms it to a random cipher text character. This process generates more strong cipher character compared to the analogous algorithms. The limitation of the algorithm is the key exchange problem which could be dealt with in future.

REFERENCES

[1] ERIC MAIWALD "Network Security: A Beginner's Guide" *Copyright © 2001 by The McGraw-Hill Companies.*

[2] 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*

[3] Lt. Ravindra Babu Kallam, Dr. S. Udaya Kumar and Dr. M. Thirupathi Reddy *"A Block Cipher Generation Using Color Substitution" published in International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 28 2010*

[4] Suryavanshi H., Dr. Bansal P., *Conference Proceedings of Ninth IEEE and IFIP International Conference on Wireless and Optical Communication Networks, IEEE ISBN: 9781467319881, IEEE DOI: 10.1109/WOCN.2012.6335543*, 2012

[5] Suryavanshi H., Dr. Bansal P., *"Design and Implementation of an Improved Cryptographic Algorithm using UNICODE and Universal Colors" published in STM Journals, Current Trends In Information and Technology, Volume 3, Issue 1, ISSN: 2249-4707*

[6] Web Reference: http://msdn.microsoft.com *[As accessed on: 22-march-2013].*

