Security using Colors, Figures and Images

Ajmal K.A.
Computer Science & Engineering
K.M.E.A. Engineering College,
Edathala, Alwaye, India

Dalton Dhavarev
Computer Science & Engineering
K.M.E.A. Engineering College,
Edathala, Alwaye, India

M. Selin
Computer Science & Engineering
K.M.E.A. Engineering College,
Edathala, Alwaye, India

V.P. Abeera
Computer Science & Engineering
K.M.E.A. Engineering College,
Edathala, Alwaye, India

ABSTRACT
The growth of technology in computer science and popularity of information technology among the common people changed the means of information exchange using mail services of paper messages to Email services of electronic messages. From the very beginning of the use of these types of technologies, the security offered by these techniques is a big question. Popular solutions for ensuring the security of electronic messages are cryptography and steganography. Steganography is the art of hiding the existence of the communication message before sending it to the receiver.

The common techniques used are – Symmetric cryptographic algorithms and substitution steganography methods. Since these techniques are popular and common, now everybody knows how these techniques ensure the security of messages. Message hackers can now easily break these techniques because of the intense experience they might have earned by handling these types of techniques. So, there exists need for new techniques and methods to ensure the security of message.

To overcome the problems associated with using the existing common and popular methods, the proposed methods use the concepts of RGB color model to hide the encrypted contents. In this method the encrypted contents are converted to a bitmap image. It has many advantages over the simple symmetric key encryption and popular LSB steganography method. The first proposed technique uses concept of color only, whereas the second method combines geometric figures with color codes to hide the message. These two methods can be considered as new techniques of generation steganography.

General Terms
Security, Algorithms, Cryptography, Encryption, Decryption, Steganography.

Keywords
Symmetric key cryptography, RGB Color model, Generation Steganography

1. INTRODUCTION
Security of information exchange and data storage always has great importance. The most common techniques used for ensuring the security are cryptography and steganography. But nowadays hackers are becoming more powerful and they earned great experience in handling the popular security ensuring mechanisms. There is always an enormous requirement for new methods to ensure the security. One of the proposed methods gives a new method to hide encrypted data in image using RGB color model concept and second method uses geographical figures and colors to implement the generation steganography.

2. BASIC OVERVIEW ON CRYPTOGRAPHY
Cryptography is the science of manipulating the data such that it is made unreadable for the unintended readers. It is the practice and study of hiding information. Modern cryptography combines the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Cryptology prior to the modern age was almost synonymous with encryption, the conversion of information from a readable state to an unreadable format. The sender retained the ability to decrypt the information and therefore avoid unwanted persons being able to read it. Since World War I and the popularity of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Modern cryptography follows a strongly scientific approach, and designs cryptographic algorithms around computational hardness assumptions, making such algorithms hard to break by an adversary. Such systems are not unbreakable in theory but it is infeasible to do so by any practical means. These schemes are therefore computationally secure. There exist information - theoretically secure schemes that provably cannot be broken - an example is the one-time pad - but these schemes are more difficult to implement than the theoretically breakable but computationally secure mechanisms. Different terms in cryptography are the following.

- Plain Text: The data to be encrypted is called as plain text.
- Cipher Text: The encrypted data obtained as a result of encryption process is called as cipher text.
- Key: Key is special information used for conversion of plain text and cipher text.
- Encryption: Process of converting plain text into cipher text.
- Decryption: Process of converting cipher text back to plain text.

Different types of cryptography methods are-Symmetric key cryptography, Asymmetric key cryptography and hash function [5].

2.1 Symmetric Key Cryptography
In symmetric key cryptography same key is used to convert plain text to encrypted text and encrypted text back to plain text. Examples of symmetric key cryptography are RC4, Data Encryption Standard (DES), and Advanced Encryption Standard (AES). Symmetric key cryptography schemes are common and popular.

2.2 Asymmetric Key Cryptography
Asymmetric key cryptography uses two keys to perform the encryption and decryption process. The sender uses a public

key to perform the encryption and receiver decrypts the message using his private key. Famous example for asymmetric key encryption is RSA encryption.

2.3 Hash Function

Hash functions are irreversible mathematical transformations. Message digest is an example for hash function.

3. BASIC OVERVIEW ON STEGANOGRAPHY

Steganography is the study of hiding data using other data. Steganography, literally "hidden writing" is nowadays most often associated with embedding data in some form of electronic media. Data is hidden by adding or altering insignificant bits of information of a file.

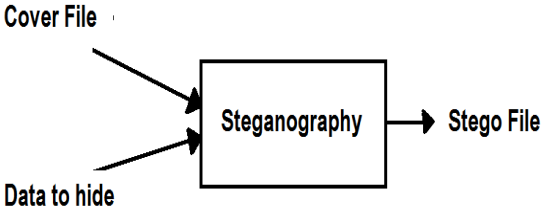

Figure 1: Steganography Application Scenario

Figure 1 illustrates a typical steganography application scenario. The application receives the data to hide as input. It may be text, audio, video or image and the file in which data will be hidden called cover file. The stego file is the result of the process. Although it contains the original cover file data as well as the hidden information, the stego file is virtually identical to the cover file. Different techniques of steganography are the following:

3.1 Injection or Insertion

In this technique, store the data you want to hide in sections of a file that are ignored by the processing application. By doing this you avoid modifying those file bits that are relevant to an end-user - leaving the cover file perfectly usable. For example you can add additional harmless bytes in an executable or binary file. Because those bytes don't affect the process, the end user may not even realize that the file contains additional hidden information. However using an insertion technique changes file size according to the amount of data hidden and therefore, if the file looks unusually large it may arouse suspicion.

3.2 Substitution

Using this approach, replace the least significant bits of information that determine the meaningful content of the original file with new data in a way that causes the least amount of distortion. The main advantage of this technique is that the cover file size doesn't change after the execution of algorithm. The drawback is, the resulting stego file may be adversely affected by quality degradation and that may arouse suspicion. Another disadvantage is that it limits the amount of data that can be hidden.

3.3 Generation

This technique doesn't require an existing cover file. This generates a cover file for hiding data. The main flaw of the insertion and substitution technique is that hackers can compare the stego file with any pre-existing copies of the cover file .When we use generation technique the result is an original file, and therefore is immune to comparison tests.

4. RGB COLOR MODEL

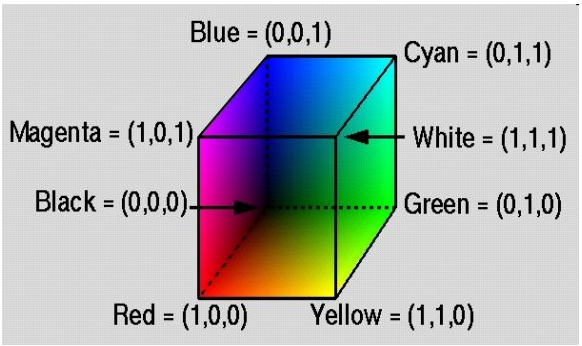

Figure 2: RGB Color Cube

The RGB color model is an additive model in which Red, Green and Blue are combined in various ways to produce other colors. By using appropriate combination of red, green and blue intensities, many colors can be represented. Typically 24 bits are used to store a color pixel. This is usually apportioned with 8 bits each for red, green and blue giving a range of 256 possible values or intensities for each hue. A color in RGB color model can be described by indicating how much of each of the red, green and blue color is included. Each can vary between the minimum and maximum. If all are minima, the result is black. If all are maxima, the result is white.

5. EXISTING SYSTEMS

- Simple symmetric cryptographic algorithms like RC4, DES and AES are commonly used.
- LSB (Least Significant Bit), a substitution steganography method is widely used for hiding data. Modifications of substitution steganography using images as cover file is also used as described in [1].
- RGB color model concept is used to assist cryptographic security. According to [2] unique receiver is identified using color.
- According to [1] -The concept of multiple cryptography- the data will be encrypted into a cipher text and the cipher text will be hidden into a multimedia image file in encrypted format. We shall use traditional cryptographic techniques to achieve data encryption and visual steganography algorithms will be used to hide the encrypted data.

6. PROPOSED METHODS

We propose two methods to increase the security of information exchange.

- Use of RGB color concept and generation steganography to increase the security of the content.
- Use of color and geometric figures to hide data by generation steganography.

6.1 Use of RGB Color Concept and Generation Steganography

6.1.1 Hiding the Message

In 32 bit bitmap file, each pixel consists of 4 bytes

1. Red
2. Green
3. Blue
4. Alpha

With RGB color model, a color can be represented as intensities of red, green and blue. Our techniques have the following steps:

1. Apply RC4 to the content we need to transfer.
2. Convert the encrypted content to byte stream.
3. Create a new bitmap file with fixed pixel width say M and height depends on size of encrypted content.
4.
   A) Set the next encrypted byte value as RED intensity of the pixel.
   B) Set the next encrypted byte value as GREEN intensity of the pixel.
   C) Set the next encrypted byte value as BLUE intensity of the pixel.
5. Repeat step 4 for M pixels.
6. If there are more than M X 3 encrypted bytes then continue step 4 after incrementing height by one and create new pixels in the new row.
7. Continue steps 4-6 for entire encrypted bytes.
8. Stop.

6.1.2 Extracting the Message

The application of the proposed method will convert the encrypted content to a 32 bit bitmap image. Now to extract the content first we need to extract the encrypted content from the image. The steps required are the following:

1. Declare a byte array with size equal to three times the number of pixels in the image.
2.
   A) Store the red intensity of the pixel to the byte array.
   B) Store the green intensity of the pixel to the byte array.
   C) Store the blue intensity of the pixel to the byte array.
3. Repeat step 2 for entire pixels in the image.
4. After step 3 the byte array will contain the encrypted content in its byte form.
5. Apply the decryption algorithm of RC4 over the encrypted bytes to read the original content.

6.1.3 Advantages

- This technique is applicable to any type of encryption algorithm.
- This hides the encrypted content. The hacker never realizes what the content is.
- Size of created bitmap file never increases marginally.
- The width or height of bitmap file can be decided by the application developer.
- Alpha can be made use in storing the encrypted byte to reduce the file size.

6.2 Use of Colors and Geometric Figures

6.2.1 Hiding the Message

Figures and colors can be combined to hide data from viewers. There are predefined functions in many languages to draw simple figure like rectangle, circle etc.

Example: rectangle(x1,y1,x2,y2); is a function in C to draw rectangle at left-top coordinate at x1,y1 and right-bottom coordinate at x2,y2 position. We can use this x1, y1, x2, y2 to store ASCII representation of 4 characters. Thus a single rectangle can used to represent 4 characters. Now consider the famous color pattern VIBGYOR. Using this VIBGYOR, first set the color to violet (V), then draw rectangle with that color to represent first 4 characters of the message. Then set color to Indigo and repeat the process. So with VIBGYOR we can represent 4X7=28 characters as 7 rectangles in 7 colors.

More proposals related to this are:

1. Choose color patterns other than VIBGYOR.
2. Rearrange the order of color pattern for each message using some keys.
3. Make use of different geometric figures like circles and rectangles.
4. The code representation (ASCII, EBCDIC et. al) can be selected.

6.2.2 Extracting the Message

Imagine that we received a bitmap file with 7 rectangles in 7 colors. The steps required to read the message are:

1. Scan the pixels to get violet pixels coordinate positions.
2. Store the violet pixels x coordinate values to an array X value and y coordinate values to array Y value.
3. Find the minimum and maximum values from X values and Y values. These minimum, maximum values corresponds to x1, x2, y1 and y2 values of the rectangle represented with violet color.
4. Store x1, y1, x2, y2 to an array ASCIIVALUE .Now this contains ASCII values of first 4 characters.
5. Repeat steps 1-4 for remaining colors in VIBGYOR.
6. Convert ASCIIVALUES content to characters to read the message.

6.2.3 Drawbacks and Existing difficulties

Drawbacks and existing difficulties in implementation:

1. Size of bitmap file to represent simple message may be larger.
2. In some cases, direct ASCII representation may prevent user from generating geometric figures with that values as parameters.(Example: rectangle(0,0,0,0)appear as line and chance of overlapping of figures cannot be eliminated.)

Even though this proposed technique have some drawbacks, it can be useful if it is studied and developed well in future.

7. RESULTS

Figure 3 shows the result obtained by applying simple RC4 encryption algorithm and figure 4 shows the result obtained by the proposed technique of use of RGB color concept and generation steganography to increase the security of encrypted content.

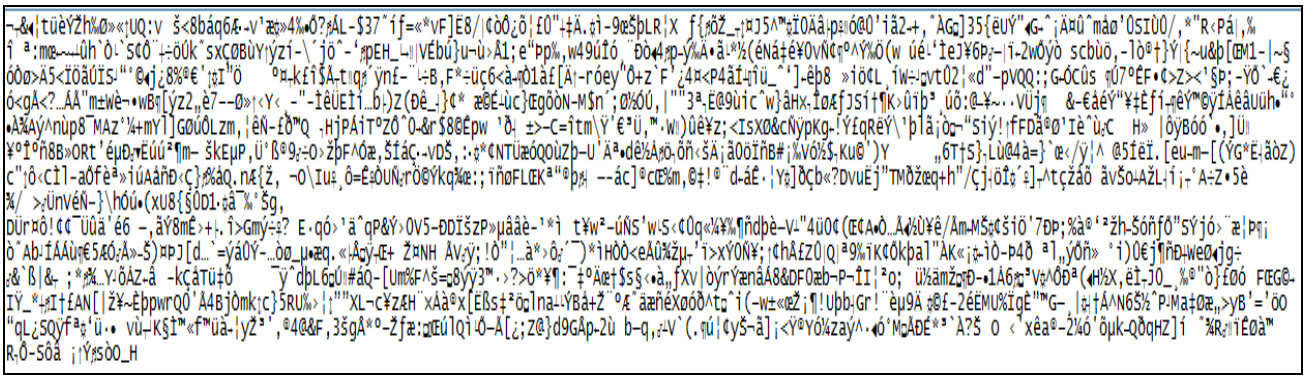

Figure 3: Encrypted content of the first page using RC4 alone

Figure 4: Encrypted content of the first page using proposed approach

8. CONCLUSION

The proposed techniques using RGB color concept and geometric figures with colors are can be considered as two implementations of generation steganography. They can be applied to plain text message to hide data as well as over some encrypted contents to increase the security further. Technique using RGB color concept with generation steganography have an advantage of not increasing the file size after its application, whereas the second technique, using geometric figures with colors creates meaningful images so that it can hide the data more effectively. Both of these effectively combine the concepts of colors and generation steganography to increase the security of confidential information.

9. FUTURE SCOPE AND APPLICATIONS

Both of the proposed methods have their future scope and applications.

9.1 RGB Color Concept and Generation Steganography

This technique has the following future scope and applications

- It can be applied and experimented for other encryption algorithms like DES, AES etc.
- The option to use the encrypted bytes as a single pixel's intensity values of RED or GREEN or BLUE or any combinations of RED,GREEN and BLUE belongs to the user; It can produce image having shades of red or green or blue only as user wants and it can reduce the arise of suspicion also.
- The above methods can be applied to other image formats like png, dib etc.

9.2 Colors and Geometric Figures

- Geometric figures like circle, line et.al, can also be used in combination with colors.
- Other color codes than the VIBGYOR can be made use of. Example: Color code to denote resistance of resistors.
- Various keys (numeric, alphabetic et.al) can be made use to manipulate the order of color codes we use to draw the geometric figures.

These methods can be used for increasing the security of information exchange made using Email services over the internet. It will be useful for top level business professionals and international defense officers to communicate with tight security. Storage of data can also be made more secured by applying these techniques. Storing data after applying these techniques is a better option than storing plain data. Since these methods will not increase the size of file after application of these methods, it will not need a larger memory to store them.

10. ACKNOWLEDGEMENTS

We would like to thank Dr. C.I.Abdul Rahiman, Director of K.M.E.A Engineering College, for his valuable support throughout the creation of this research paper. We express our sincere and heartfelt thanks to Dr. V.G.Rajesh, our principal for providing us the right ambience for carrying out this work.

11. REFERENCES

[1] Piyush Marwaha and Paresh Marwaha. 2010. "Visual cryptographic steganography in images", Second International conference on Computing, Communication and Networking Technologies.

[2] S.PavithraDeepa, S.Kannimuthu and V.Keerthika. 2011. "Security using colors and Armstrong numbers", Innovations in Emerging Technology (NCOIET), National Conference.

[3] Liu F., Wu C.K., Lin X.J. 2008 "Color visual cryptographic schemes", IET journals

[4] Paresh Marwaha, Piyush Marwaha and Shelly Sachdeva. 2011 "Content based Image Retrieval in Multimedia Databases", International Journal of Recent Trends in Engineering.

[5] Khalifa O.O., Islam M.D.R., Khan, S., Shebani M. 2004 "Communications Cryptography", RF and Microwave Conference, 2004.

[6] Debashish Jena. 2009 "A Novel Visual Cryptography Scheme", IEEE International Conference on Advanced Computer Control.

[7] Yongzhen Zheng, Fenlin Liu, Chunfang Yang, Xiangyang Luo, Kun Zhao. 2011. "Identification of steganography software based on core instructions template matching", IEEE Conference Publications.

[8] Huaxiong Zhang, Jie Hu, Gang Wang, Yu Zhang. 2011. "A steganography based scheme on fractal images".

Second International Conference on Network and Distributed Computing.

[9] Sarreshtedari S, Ghotbi M., Ghaemmaghami S. 2009. "One –third probability embedding: less detectable LSB steganography". IEEE International Conference on Multimedia and Expo.

[10] Chanu Y.J., Tuithung T., Manglem Singh K. 2012. "A short survey on image steganography and steganalysis techniques". National Conference on Emerging Trends and Applications in Computer Science.

[11] Atul Kahate, "Cryptography and Network Security", Tata McGraw Hill Publications.

[12] William Stallings, "Network Security Essentials-Applications and Standards", Pearson Education publications.