Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(RESEARCH ARTICLE)

Check for updates

Using mono chrome image in secure data transfer based on book cipher

Hind Jumaa Serteep * and Wedad Abdul Khuder Naser

Computer since department, Al-Mustansiriyah University, Ministry of Higher Education and Scientific Research , Iraq.

Global Journal of Engineering and Technology Advances, 2022, 11(01), 045–051

Publication history: Received on 16 February 2022; revised on 24 March 2022; accepted on 26 March 2022

Article DOI: https://doi.org/10.30574/gjeta.2022.11.1.0058

Abstract

In the current digitalized world human race confront huge and fast technical progress in communication networks, That contribute to exposure of data and information that is transmitted through these networks to different levels of exposure and attack Also, the authentication of the digital products and services become very important to both makers and customers and can be separated from those that are invalid , The science of transfer secret data in several multimedia carriers like audio , text, video or image so that can achieve the authentication requirements that were mentioned is called steganography. This paper introduces a new steganography technique that will increase the difficulty of exhaustive key search, it based on book cipher combined with ASCII (American Standard for Information interchange) mapping technique using image as reference key.

Keywords: Book cipher; Monochrome Image; Image; ASCII; least significant bit

1. Introduction

Today the advent of internet technology with its endless services bring a big concern which is how to provide a secure connection between entities [1]. Cryptography techniques attract many researchers to transform their original message plain text from its comprehensible to incomprehensible form by applying a secure shared key to the plain text to generate the cipher text [2]. This encrypted message cannot be decrypted without applying a secure shared key that is known between the authorized individuals (sender and receiver) [3].

Cryptography algorithms can be classified into different types such as stream cipher, block cipher, conventional and public key cryptography. Some of these algorithms are sophisticated, creative, and need mathematical computation [4].

Steganography, originated form Greek language, an ancient art for information protection. “stegos” implies “cover” and “grapy” refers to “writing “that is known as covered writing [5].by using steganography the confidential information is concealed this will provide higher level of protection [1]. In cryptography the encrypted message could lead to suspicion while the hidden information can not reveal any doubt because no one except the authorized partners could infer the existence of information.one of the most important application of steganography is in providing copyright for digital media document traffic [6].

Watermarking is the insertion of imperceptible piece of code to embed information inside an image. it acts as a digital signature to the legal owner that can give the hidden messages to proof his ownership.

It can be concluded that cryptography algorithm is used to modify the message content but the presence of the message is left as is it. But the purpose of steganography is to stow away transmitted information imperceptibly [7].

* Corresponding author: Hind Jumaa Serteep
Computer since department, Al-Mustansiriyah University, Ministry of Higher Education and Scientific Research , Iraq.

2. Infra-structures

2.1. Monochrome Image

There are many other names for the monochrome image for example bi-level image , two level image , the pixel value of this kind of image is either (0) for represent black color or (1) for represent white color , for that the monochrome image showed as black and white image.

The generation of the monochrome image depend on the threshold value of gray-scale image, the value of monochrome image pixel generated by compare of gray scale image pixel value with the threshold value, if it is greater than the threshold value the monochrome image pixel turn in to white and if it less than the threshold value it turn in to black [8].

The Monochrome images often a rise in digital image processing as masks or as result of certain operation such segmentation, thresholding and dithering. Some input / output devices such as laser printers and fax machines, in our paper we try to add another usage of monochrome image beside to what we mention, we will use monochrome image in the secure data transfer through communication network.

2.2. Book Cipher

Book cipher is an encryption method where use a book or some piece of text as a encryption key, the operation principle of the book cipher depend on taking the words (one by one) of the secret message and compare it with the words of the encryption key and when find match replace that word from the secret message by the location of the matching word form the key, In general case it is necessary that the sender and the receiver should have the same book and the same edition also[9], ,if there is a word in the secret message don't have a match in the encryption key , in this case the encryption is done by splitting the unmatching word in to litters and start replacing litters instead of a complete word . In this paper we planning to reuse this old encryption method by giving computerized touch to book cipher for eliminating the limitations that make it outdated and to overcome this issue [3]. The book cipher has long history, it development over a period of the last 400 years [10], The Dukes of Wellington army Geroge Scovell utilized this encryption technique in several campaigns of the Peninsular War (AD1807-1881), also it's used as a guaranteed way for exchange information in the cold war period [3].

3. The proposed method

The approach that has been proposed come from the book cipher primary concept by replace the bit of the plane text with the pixel location of the reference key (Image).

Two users (User A and User B) has been agree that to use a certain images with dimensions (m,n) as there reference key , and each one know the reference key of the other side user (each other), User A will perform the following steps to encrypt the secret message.

- Divide the words of the secret message in to individual alphabets.
- Convert each alphabet to numerical number depending on the ASCII table.
- Convert the ASCII numerical value of each alphabet to binary number (byte).
- The binary value of each alphabet spilt to bit segments (1 bit, 2 bit, or 4 bit) segments
- User A create monochrome image with dimensions equal to dimensions of its reference key and make the color of all pixels black.
- User A Separate the color channel of the reference key and convert the numerical value of each pixel to binary
- The matching process done by changing some pixel color of the monochrome image created in step 6 pixel from black to white the location of the white pixel depend on the result of the matching process, that process start by take the first segments (1 bit for example) of the first secret message alphabets and match it with the LSB (least significant bit) of one color channel of the encryption key (Image) , when matching found at certain pixel the location of that pixel used to change the color of the monochrome image pixel
- Take into consideration the matching process for the 2nd segment bit of the 1st alphabet will continue from where it's found first match in the reference key.
- This process will continue until the last segments of the last alphabets of the secret message.

- User A will send only the result monochrome image that comes out form the matching process to User B. (See Figure 2).

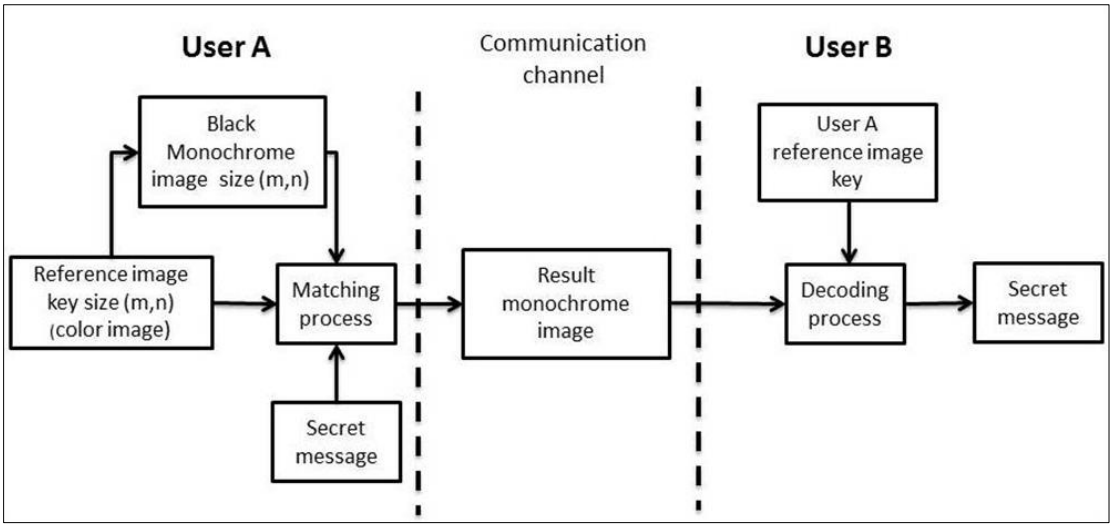

Figure 1 The proposed method diagram

User B will do the following steps to decode the received monochrome image to obtain the secret message.

- Read the Monochrome image
- Split the reference image in to three color channel (Red, Blue and green).
- Convert the pixel numerical number of the (agreed color channel) to binary number (Byte).
- From the monochrome image when found white pixel use it location to obtain the LSB from pixel binary value of the reference key image color channel.
- Step 4 repeat until finish reading of the received monochrome image.
- Result from steps 4 & 5 is a long string to bits, every 8 bit are combined to form a byte , transform each byte to numerical value , and then for the ASCII table User B can convert these number in to alphabets and but that User B will get the secret message.

4. Discussion

In the section we will validate our proposed method, this evaluation will see the effectiveness of the proposed method and study it action against tradition book cipher decline reason.

The decline reasons of the tradition book cipher are address as follows:-

- Reference Key a huge data base of digitalized books must by stored on all users that use tradition book cipher that will be not necessary to our method because there are an infinite supply of digitalized images available online and even the user have to store the images it will be no bigger than the digitalized books .
- Language , knowing the language of the tradition book cipher users by the attacker will made the brute force attack easier, that have no effect on our method because our proposed method reference key is image no a book.
- Symbols encryption, addressing of the space between word and other symbol like (%, ! , @ … etc) is difficult in book cipher but in our proposed method is easy because every symbol have ACSII code.
- If a word from the secret message text does not exist in the reference book key, then that particular word is divided into syllables, and these corresponding syllables are coded, our proposed method can easily overcome this because it does not search words but us search and compare bits.

5. Results

The proposed method was implemented and tested by using Visual Basic 2013 as programing language , the program was built in personal computer has 8.1 windows operation system, This technique accepts various image size and types (JPEG , PNG , BNP , …..etc)

To clarify the proposed technique and to show the action improvement that adding to book cipher, the following case study has been shown, the text below is the clear text to be encoded by our proposed technique.

The input of the proposed technique will be Clear text (book, paper, Cars) as secret message and some different reference images as reference keys.

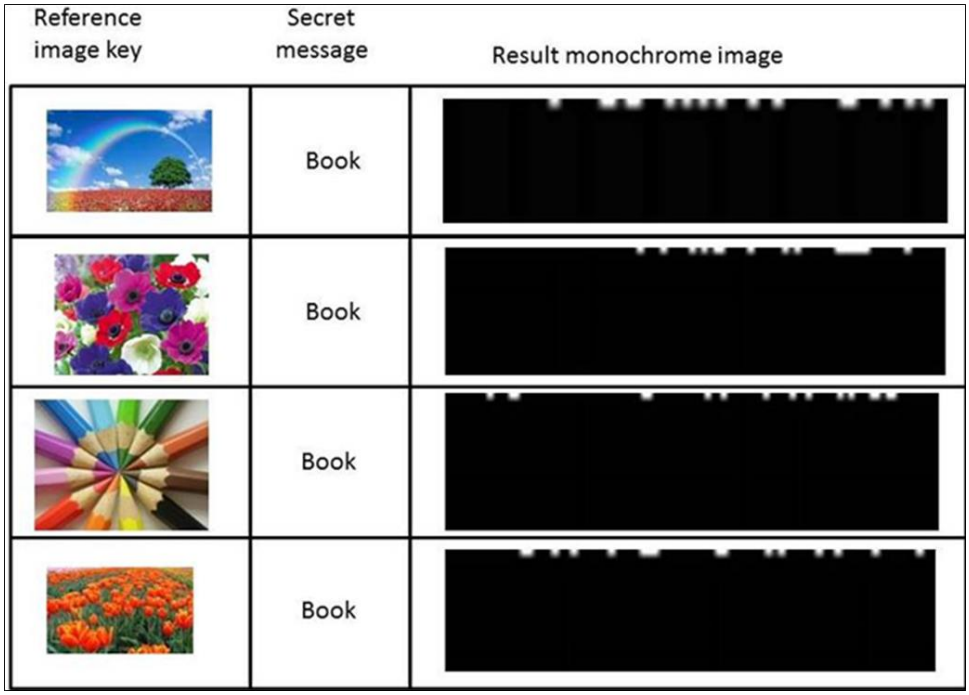

Figure 2 Result monochrome image from different reference images

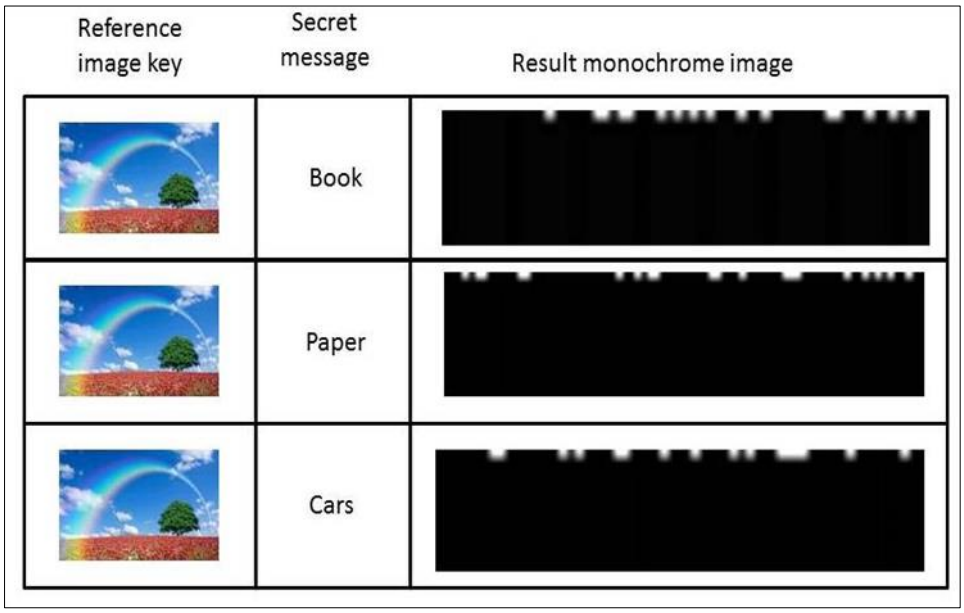

Figure 3 Result monochrome image for different reference images

Figure #2 above shows the encryption of the clear text (Book) as seen that the proposed technique generate different monochrome image for the same secret message from different reference images key. Figure#3 below shows that proposed technique generates different monochrome images for different secret messages from same image reference key, form that it's clear that if the other side didn't use the correct reference key image to decode the monochrome image he won't receive the correct secret message.

6. Comparison with the precedent techniques

Below a comparison has been display with some existing techniques

6.1. Text steganography using changing word spelling [11]

The author suggest a secret message concealment way by placing the US word for concealment 0 and UK word for concealment 1.

6.2. Text steganography by inter word spacing paragraph spacing approach [12]

The developers of this technique introduce a method to shift the paragraph lines of the text vertically to some degree (like the line moved 1/300 inch vertically) of the words of any line are shifted horizontally and the data are covered up by making unique shape of the text.

6.3. Text steganography by using letter points and extensions [13]

In this method the Arabic language is used to embed any secret message by using pointed letter to hold 1 and un pointed letter to hold 0

Table 1 Comparison of our method with other methods

Method name	No of Embedding Bits:	Changes Occurred	Embedding Capacity	Similarity Measure
Text steganography using changing word spelling [11]	Single (0 or 1)	In Word (US for 0 , UK for 1)	the embedding capacity of this method is the lowest compared to the other methods because it used a whole word to embed bit 0 or bit 1	Not Applicable
Text steganography by inter word spacing paragraph spacing approach [12]	single (0 and 1)	In line , word or paragraph.(one space for 0 , two space for 1)	Greater that Method 1 lesser than method 3 , method 5 because here increasing the white spaces embedding capacity can be inversed but this increasing can also be done at some extent. Otherwise it will be easy to trace the changes made in the text	Not Applicable
Text steganography by using letter points and extensions [13]	single (0 and 1)	In letter (pointed letter for 0 , unpointed letter for 1	Greater than method 1 and method 2 but lesser than method 4 and method 5 because it changes a single letter to embedding a bit 0 or bot 1	Not Applicable
Hiding data in text through changing Alphabet patterns (CALP) [14,15]	Double (00,01,10,11)	in letter (changing letter pattern)	Greater than the previous three methods because one change of letter embed two bits simultaneously.	0.99
Hiding Data in text using ASCII Mapping Technology (AMT) [16]	Single bit and double bit can be implemented	In ASCII. This is not visible to human eye.	Same as CALP	0.9885
Using Mono chromo image in secure data transfer depending based on book cipher	(1 bit, 2 bit, or 4 bit) can be implemented	black pixel change to white pixel in full black mono chrome image	Greater than the previous four methods because it depend on image size (length and width) , as the size of image increase allow to embedding more text	Not Applicable

6.4. Hiding data in text through changing Alphabet patterns (CALP) [14,15]

The author take the advantage of making some changes in the English language to hold 00 , 01, 10 , 11 for embed the secret message

6.5. Hiding Data in text using ASCII Mapping Technology (AMT)[16]

The author utilize the English language to embed any secret message without altering the letter pattern. Extra level of security is achieved by quantum logic. Authentication of the secret message can also be tested.

By checking table #1 below it is seen that our proposed technique is superior to other techniques as far as embedding capacity and robustness, and also our method is not limited to the English language, but can be applied to other international languages.

7. Conclusion

The current paper present new method for point to point data transfer application by compare bits of the clear text with the least significant bit of image pixel. The new method attain two interesting point , the first point is there is no change occur in the reference key image because that image is key for encode and decode the secret message , another important point is that this new method depend on infinite key space as there is huge large number of image available on the web.

Compliance with ethical standards

Acknowledgments

After completing this research, I thank God Almighty and the Department of Computer Science at the College of Education (Al-Mustansiriya University) and my family for completing this research.

Disclosure of conflict of interest

Authors declare no conflict of interest.

References

[1] Reza tavoli , Maryam bakhshi , Fatemeh salehian , A new Method For Text Hiding In The Image By Using LSB, International Journal Of Advanced Computer Science And Application. 2016; 7(4): 126-132.

[2] Saraju P Mohanty. Digital Watermarking: A Tutorial Review. Department of computer science and Engineering, University of South Florid. 1999.

[3] Rasike Lele, Rohit Jainani, Vihang Mikhelkar, Aniket Nada, Mrs. V Meshram. The Book Cipher Optimised Method To Implement Encryption And Decryption, International Journal Of Scientific & Technology Research. 2014; 3(1): 11-14.

[4] Weigi luo, Jiwu Huang, Fangiun Huang. Edge Adaptive Image Steganography Based on LSB Matching Revisited, IEEE Transactions On Information Forensics And Security. 2010; 5: 201-214.

[5] Vijaya Raghave Kukapalli, Tarakeswara Rao, Satyanarayana Reddy. Image Steganography By Enhanced Pixel Indicator Method Using Most Significant Bit (MSB) Compare, International Journal of Computer Trends and Technology (IJCTT). 2014; 15: 97-101.

[6] Budda Lavanya, Yangala Smruthi, Srinivasa Rao Elisala. Data Hiding In Audio By Using Image Steganography Technique, International Journal Of Emerging Trends & Technology In Computer Science (IJETTCS). 2013; 2: 27-30.

[7] Changda Wang, Shiguang Ju. Book Cipher with Infinite Key Space. International Symposium on Information Science and Engineering (ISISE). 2008; Pages: 456-459.

[8] Albert C Leighton, Stephen M Matyas. The History of book cipher, Springer – Verlag , Berlin Heidelberg. 1985.

[9] Mohammed Shirali-Shahreza. Text Steganography by Changing Word Spelling, International Conference on Advanced Communication Technology (ICACT). Feb 2008; Pages: 1912-1913.

[10] LY Por, B Deline. Information Hiding: A New Approach in Text Steganography, 7th WSEAS international Conference on Applied Computer and Applied Computational Science (ACACOS '08). April 2008; 689-695.

[11] Gutub A, Fattani MM. Text Steganography by Using Letter Points and Extensions World Academy of Science, Engineering and Technology. 2007; 27: 13-27.

[12] Souvik Bhattacharyya, Pabak Indu, Sanjana Dutta, Ayan Biswas, Gautam Sanyal. Hiding Data in Text through Changing in Alphabet Letter Patterns (CALP). Journal of Global Research in Computer Science (JGRCS), March 2011; Volume 2, No 3: Pages 33-39.

[13] Souvik Bhattacharyya, Pabak Indu, Sanjana Dutta, Ayan Biswas, Gautam Sanyal. Text Steganography using CALP with High Embedding Capacity, Journal of Global Research in Computer Science (JGRCS). May 2011; Volume 2 , No.5 : Pages 29- 36.

[14] Souvik Bhattacharyya, Pabak Indu, Gautam Sanyal. Hiding Data in Text Using ASCII Mapping Technology (AMT), International Journal of computer Application (0975-8887). May 2013; Volume 70 , No.18 : Pages 29-37.

[15] Rafael C. Gonzalez, Richarad E. Woods. Digital Image processing (3rd edition), Pearson Education. 1993.

[16] Scott E Umbaugh. Digital Image Analysis and Processing (2nd edition) ,CRC Press , Taylor & Francis Group , 2013.