JOURNAL OF COMPUTATIONAL INNOVATION AND ANALYTICS
https://e-journal.uum.edu.my/index.php/jcia

How to cite this article:
Osman, B., Yahya, N. I., Mohd Zaini, K., & Abdullah, A. (2023). Text Steganography Using the Second Quotient Remainder Theorem and Dark Colour Schemes. *Journal of Computational Innovation and Analytics, 2(1),* 21-40. https://doi.org/10.32890/jcia2023.2.1.2

TEXT STEGANOGRAPHY USING THE SECOND QUOTIENT REMAINDER THEOREM AND DARK COLOUR SCHEMES

[1]Baharudin Osman, [2]Noor Izzah Yahya,
[3]Khuzairi Mohd Zaini & [4]Azizol Abdullah
[1,2&3]School of Computing, Universiti Utara Malaysia
[4]Faculty of Computer Science and Information Technology,
Universiti Putra Malaysia

[1]Corresponding author: bahaosman@uum.edu.my

Received: 12/07/2022 Revised: 12/09/2022 Accepted: 16/11/2022 Published: 30/1/2023

ABSTRACT

Data communication over the Internet has increased significantly, resulting in high data traffic and concerns over data security. Information sent over the Internet always gets the attention of intruders, which causes the effort to increase the security of sensitive data and the need to prevent leakage. Steganography is one of the techniques to protect the confidentiality of data that can be accomplished by hiding secret information within the medium of text, images, audio, and video. Hiding a secret message using text steganography can be done on character properties such as size, colour, style, etc. Colour-based steganography has always raised suspicions about the generated stego text, which is a major issue in this study. Therefore, the Red, Green, and Blue (RGB) colour technique and the Second Quotient Remainder Theorem (SQRT) were introduced in this study to perform the hiding process. RGB (0,0,0) to RGB (15,15,15) colours were used for the hiding process to avoid colour suspicion. In addition, the pseudorandom number generator (PRNG) was also used to generate dynamic hidden messages with Homophonic table generation. The results showed that the secret message can be represented dynamically and has increased the hiding capacity to 77.4%. Other than that, the selected colour has successfully avoided the suspicion of the generated stego text. Hence, the results suggested that SQRT could be employed as a method in text steganography for securing information.

Keywords: Homophonic table, RGB colour, Second Quotient Remainder Theorem, Text Steganography.

INTRODUCTION

In the current era, data transmission in digital communication plays a vital role in daily life. The Internet is a major platform widely used to exchange various forms of information such as text, images, audio, video and network protocol. Transmitting confidential information requires an efficient security system for data preservation. Data communication over the Internet has increased significantly, resulting in high traffic and concerns about the security of transmitted data (Jan, Parah, Hussan, & Malik, 2022; Mahato, Khan, & Yadav, 2017). Moreover, information transmitted over the Internet always catches the attention of intruders, which causes the security of sensitive data (Majeed & Sulaiman, 2021; Maniriho & Ahmad, 2017), and it is a severe problem and needs to be preserved to prevent leakage (Bhat, Prabhu, & Renuka, 2017; Jan et al., 2022; Joseph & Vishnukumar, 2015). Therefore, it is necessary to protect sensitive data so irresponsible parties cannot access it (Pujari & Shinde, 2016).

Due to the possibility of attacks and unforeseen changes during an active transmission across an unsafe network, it is challenging to establish trustworthy communication between two parties that share personal data (Khan, Algarni, Fayomi, & Almarashi, 2021). Failure to ensure that the information sent is protected can result in it being tampered with by irresponsible parties. Hence, confidentiality and data integrity are required to protect the confidentiality of data (Babu,

2010) and ensure that the data received is not altered by third parties to protect data authenticity and originality. Information hiding is an alternative method that can be utilised to protect data because the message sent is not only encrypted, but also the existence of the message is not noticed by an intruder during the data transfer process (Baawi, Mokhtar, & Sulaiman, 2018; Zhang, Huang, Wang, Lin, & Gao, 2017). Similarly, Krishnan et al. (2017) suggested that steganography is one of the techniques that can be used to overcome this problem.

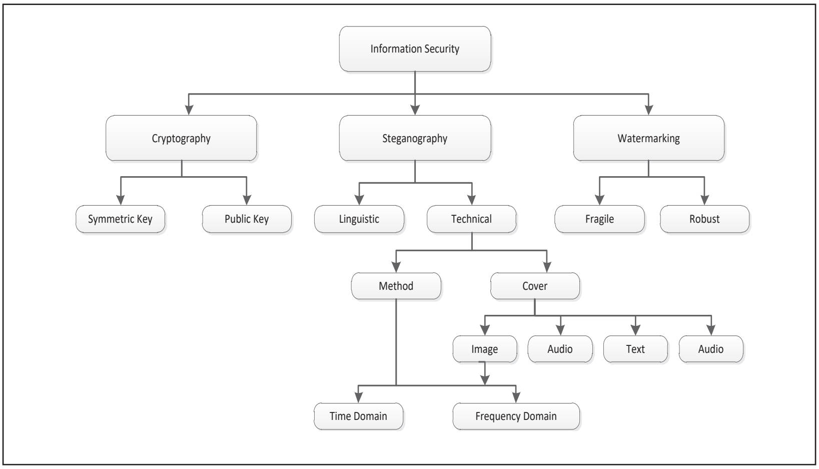
This study identifies two key issues that make people suspicious of the generated stego text: the static representation of secret message characters and significant colour changes to the generated stego text (Ahvanooey, Li, Hou, Rajput, & Yini, 2019). In order to minimise noticeable colour changes to the generated stego text, the major goal of this study is to recommend using specific values for each Red, Green, and Blue (RGB) colour. In addition, this study also suggested a technique for dynamically representing secret messages based on the placement of randomly chosen characters. In order to generate secret message characters dynamically, homophonic cypher tables were generated based on the cover text. Additionally, it is proposed to use the Second Quotient Remainder Theorem (SQRT) to map the values of (x, y, and z) to RGB colours to transform the secret message characters into a three-dimensional (3D) representation form.

RELATED STUDIES

Information security is an essential issue in the context of protecting user information. It can be classified into steganography, cryptography and watermarking, which are the methods used to protect information. These methods are classified in Figure 1 (Amirthrajan & Rayappan, 2013).

Figure 1

Information Security Systems Classification (Amirthrajan & Rayappan, 2013)

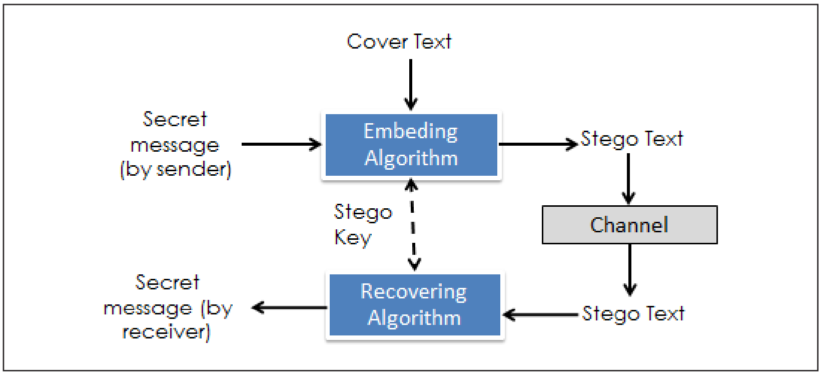


Cryptography is the process of converting the original message into plaintext, and the result generated is known as ciphertext. It is in the form of unreadable characters and suspicious code. Meanwhile, steganography is a method to hide a secret message in a particular medium, such as text, image, audio or video (Agath, Sidpara, & Upadhyay, 2018; Jan et al., 2022). The message is hidden in the cover text, and the final result of steganography is called a stego text. The generated stego text can be read by anyone without being aware of a hidden secret message (Joseph & Vishnukumar, 2015) and can avoid suspicion. According to Bhat, Prabhu and Renuka (2017) and Zielińska, Mazurczyk and Szczypiorski (2014), steganography can avoid the suspicions inherent in the message sent as it is more difficult and complex to identify the actual secret message as compared to cryptography. On the other hand, the watermark is the process of hiding markers such as labels, signatures or copyrights in digital media such as text, audio, video and images (Alotaibi & Elrefaei, 2018). Note that it is commonly used for copyright or trademark protection (Kumar, Malik, Singh, & Chand, 2016). Markers incorporated into digital media can be seen with the naked eye or vice versa (Douglas, Bailey, Leeney, & Curran, 2018). They cannot be easily altered (Atoum, 2018), in contrast to steganography, where invisibility is a primary concern. Most of the daily documents are sent in the form of black and white colour. There are very few cover texts that use colour text in daily documents. Thus, the scope of this research focused on black and white cover text.

Steganography involves embedding a secret message into the cover text to generate a stego text and extracting the generated stego text to obtain the original message. Figure 2 presents the primary mechanism of the text steganography process. Firstly, a secret message (or embedded data) will be concealed in a cover text by applying an embedding algorithm to produce a stego text. The stego text will then be transmitted to a receiver via a public network or communication channel. Here, the receiver needs to use a recovering algorithm parameterised by a stego key to extract the sender's secret message. A stego key is used to control the hiding process to restrict the embedded data's detection and/or recovery to parties who know it (Petitcolas, 1999).

Figure 2

The Text Steganography Components (Por & Delina, 2008)



Altering the properties of the cover text is a crucial issue in steganography (Shivani, Yadav, & Batham, 2015). Some examples are changes in the content or structure of file size, style, type, colour, shape, text format, and sentence changes. Other than that, concealing a message using colour attributes can cause significant changes and produce suspicious stego text if the use of colour is not considered. According to Rasmi and Mohanapriya (2016), an excellent steganographic method must not change the attributes of the cover medium (colour, font, style, size, background, etc.) significantly after the occurrence of the concealment process. In addition to RGB colour, most studies hide messages at sequential locations that facilitate steganalysis techniques to identify hidden messages' locations. Therefore, this paper focuses on text-based steganography by hiding messages against character colors as well as using a random location approach.

Steganography is an alternative way to provide an efficient security system so that confidential documents are not easily translated when they are spread (Agath et al., 2018) as well as do not arouse suspicion by human visual systems (Ahvanooey, Li, Hou, Rajput, & Yini, 2019). It is utilised in various fields, such as military, medical diagnosis, business-related information, and finance, to name a few (Malik, Sikka, & Verma, 2017). Steganography can hide secret messages using mediums such as images, audio, video and text. However, according to Arya and Sony (2018) and Malik et al. (2017), text-based information hiding is a hot topic and much-discussed compared to other steganography mediums because text medium uses less memory and can be achieved with low bandwidth (Arya & Soni, 2018; Malik et al., 2017). Hiding capacity is one of the measurements used in steganography to measure the performance of a stego text using Equation 1.

$$Hiding\ Capacity = \frac{Total\ bits\ of\ hidden\ message}{Total\ bits\ of\ cover\ text} \tag{1}$$

Increasing the capacity of a secret message while retaining invisibility is the primary concern of the researchers. Although many studies have been done, it is still a challenge in text steganography techniques, and the gap is still there underlying the issues of limited capacity and invisibility (Thabit, Udzir, Yasin, Asmawi, & Gutub, 2022). Table 1 shows the hiding capacity using RGB colour-based steganographic studies. This research discovered that the highest hiding capacity employing RGB colour was 94.57%, performed by Thabit et al. (2022). Nevertheless, the stego text produced by this study raises suspicion because the RGB colour used is in the range of (0,0,0) to (255,255,255), as presented in Figure 4.

Table 1

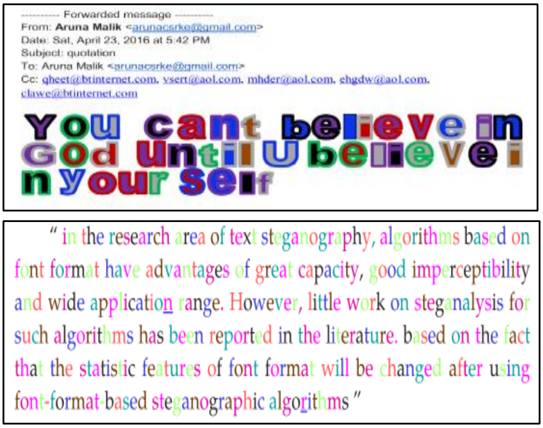
Hidden Message Capacity of Previous Studies using RGB colour

Researchers	Hidden message size (characters)	Size of cover text (characters)	Hiding capacity %
Al-Asadi & Bhaya (2016)	2 bits	7	3.57
Malik, Sikka, & Verma (2016)	198	847	13.43
Malik et al. (2017)	198	847	18.34
Al-Azzawi A. F. (2018)	34	202	25.50
Thabit et al. (2022)	801	847	94.57

RGB colour attributes have been used in text steganography in various ways. For example, formatting the character colours (Al-Asadi & Bhaya, 2016; Singh, Diwakar, & Upadhyaya, 2014; Thabit et al., 2022), formatting the character colours and underlining the colours (Wang & Li, 2014), and using blank space colours, page and paragraph margin colours (Stojanov, Mileva, & Stojanovi, 2014). There is also a combination of characters and underlined colours (Tang & Chen, 2013). Various RGB colours applied range between (0,0,0) to (255,255,255). The use of multiple RGB colours has caused the generated stego text to be suspicious, as in the study conducted by Malik et al. (2016), Malik et al. (2017) and Thabit et al. (2022). Figure 3 and Figure 4 illustrate examples.

Figure 3

Text Steganography using Malik et al. (2016) and Malik et al. (2017)



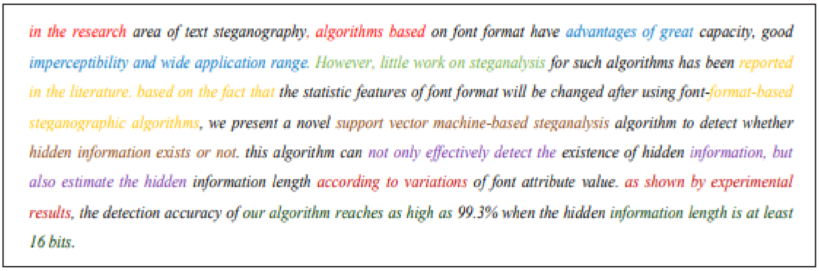
---------- Forwarded message ----------
From: **Aruna Malik** <arunacsrke@gmail.com>
Date: Sat, April 23, 2016 at 5:42 PM
Subject: quotation
To: Aruna Malik <arunacsrke@gmail.com>
Cc: qheet@btinternet.com, vsert@aol.com, mhder@aol.com, ehgdw@aol.com, clawe@btinternet.com

You cant believe in GOd Until U believe in your self

" in the research area of text steganography, algorithms based on font format have advantages of great capacity, good imperceptibility and wide application range. However, little work on steganalysis for such algorithms has been reported in the literature. based on the fact that the statistic features of font format will be changed after using font-format-based steganographic algorithms "

Figure 4

Stego Text Produced by Thabit et al. (2022)



in the research area of text steganography, algorithms based on font format have advantages of great capacity, good imperceptibility and wide application range. However, little work on steganalysis for such algorithms has been reported in the literature. based on the fact that the statistic features of font format will be changed after using font-format-based steganographic algorithms, we present a novel support vector machine-based steganalysis algorithm to detect whether hidden information exists or not. this algorithm can not only effectively detect the existence of hidden information, but also estimate the hidden information length according to variations of font attribute value. as shown by experimental results, the detection accuracy of our algorithm reaches as high as 99.3% when the hidden information length is at least 16 bits.

Malik et al. (2016) used 32 multi-colours to perform a hiding process where each colour can hide 6 bits of a secret message. Furthermore, the border and inner colour of the character are used to hide the message, whereas each character can hide 12 bits of hidden messages. Furthermore, Malik et al. (2017) used Huffman compression techniques and RGB colour coding for the hiding process using eight colours, which were divided into two groups to represent bits 0 (Fluorescent Pink, Forest Green, French Blue, French Puce) and 1 (French Lime, Fuzzy Wuzzy, Dark Cyan, Deep Magenta). Both of these studies clearly show colour suspicion of the generated stego text. Among other researchers who use RGB colour techniques in the concealment process are Al-Al-Asadi and Bhaya (2016) and Al-Azzawi (2018). However, the stego text produced by the researchers is still suspicious and produces low hiding capacity.

METHODOLOGY

The data set from Reuters-21578 was utilised as a cover text and secret messages used by researchers in the field of text categorisation (Aghdam, Ghasem-Aghaee, & Basiri, 2009; Maiti & Samanta, 2010). This study generates a Homophonic table based on the cover text to store all character locations, as shown in Table 2. Homophonic ciphers differ from Monoalphabetic ciphers in that each character can be represented with multiple representations as well as it is more difficult and complex to be analysed by intruders (Patel & Patro, 2017). Note that this technique uses the concept of one-to-many mapping, where the advantage is that a secret message character can be represented with multiple representations (Dhavare, Low, & Stamp, 2013).

Homophonic ciphers are usually used to encrypt a secret message and by the American Cryptogram Association (ACA) to represent a character in various values.

Table 2 exhibits a generated Homophonic table in which each character could be represented by multiple values, such as character “A”, represented by various values: 6, 19, 26, 32, 47, 49, 52, 57, 79, 122, 125, 126, 133, 143, 161, 168, 189, 243, 264, 268, 271, 284, 295, 336, 343, etc. This study employed these values to represent a value for a secret message obtained from a cover text with a different cover text to obtain a different value.

Table 2

Homophonic Tables

Character	Represented value
A	6,19,26,32,47,49,52,57,79,122,125,126,133,143,161,168,189,243,264,268,271,284,295,336,343,354,362,365,376,420,438,483,488,493,495,532,536,568,578,587,594,601,611,612,622,630,689,693,739,743,750,762,769,776,781,793,805,810,815,819,821,823,836,864,906,910,926,928,930,937,953,962,964,987,1006,1021,1026,1054,1069,1073,1082,1101,1126,1128,1131,1138,1169,1185,1189,1194,1199,1212,1219,1226,1236,1241,1245,1261,1273,1276,1313,1338,1347,1363,1378,1386,1407,1433,1436,1444,1450,1459,1501,1512,1548,1578,1580,1589,1606,1615,1620,1624,1648,1653,1655,1667,1670,1681,1685,1699,1704,1718,1728,1749,1751,1757,1765,1773,1777,1783,1794,1798,1801,1820,1824,1829,1832,1837,1845,1850,1860,1872,1878,1880,1887,1893,1904,1913,1915,1919,1926,1933,1948,1963,1972,2015,2024,2027,2040,2050,2053,2054,2062,2066,2088,2098,2122,2135,2140,2146,2148,2158,2165,2175,2176,2178,2183,2203,220
B	56,69,100,121,167,172,308,593,676,713,756,835,869,916,952,1042,1091,1102,1109,1175,1346,1385,1413,1426,1432,1469,1560,1705,1793,1808,1859,1924,1964,2026,2049
C	13,17,82,118,129,148,236,273,296,301,404,416,429,477,480,501,514,555,563,597,637,655,667,670,679,733,772,806,829,843,876,945,996,1051,1086,1116,1141,1235,1238,1246,1247,1256,1259,1262,1263,1303,1332,1420,1458,1490,1499,1541,1605,1614,1617,1625,1626,1635,1638,1656,1657,1678,1726,1733,1775,1896,1906,1934,1978,1985,1988,2037,2067,2090,2134,2163

(continued)

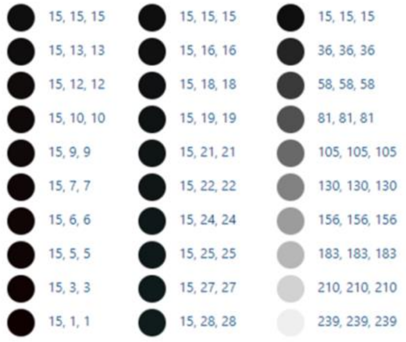
Character	Represented value
D	46,128,181,212,269,298,299,329,337,358,363,543,552,621,700,708,741,768,771,792,831,931,932,934,948,960,971,975,978,1009,1013,1016,1071,1090,1133,1151,1155,1158,1244,1250,1275,1278,1290,1360,1443,1453,1508,1536,1557,1582,1584,1623,1629,1669,1672,1720,1721,1762,1805,1847,1876,2017,2094,2102,2160,2167,2170
E	3,9,15,22,28,31,67,73,81,83,99,105,110,116,130,140,147,164,180,196,205,213,234,237,262,281,297,300,305,335,350,352,357,361,378,388,414,424,428,433,441,454,469,472,476,479,486,491,502,504,527,539,544,551,567,577,584,598,608,620,652,666,669,673,684,696,701,710,722,727,731,755,760,764,780,785,791,802,807,830,834,839,842,851,887,909,933,940,941,944,947,951,969,976,995,1002,1008,1014,1025,1043,1047,1050,1053,1062,1064,1067,1076,1084,1092,1105,1137,1140,1156,1168,1176,1181,1198,1209,1222,1243,1258,1286,1289,1316,1341,1345,1359,1362,1384,1431,1442,1454,1483,1485,1488,1493,1507,1521,1526,1530,1540,1544,1551,1570,1572,1593,1596,1604,1611,1613,1622,1637,1645,1693,1707,1712,1722,1725,1739,1741,1760,1761,1769,1792,1804,1809,1812,1819,1836,1842,1852,1858,1864,1866,1869,1875,1891,1895,1900,1918,1925,1950,1960,1968,1977,1980,1984,1987,1993,1997,2012,2020,2033,2061,2071,2073,2085,2097,2115,2126,2142,2150,2152,2173,2187,2191,2195,2202
F	78,253,391,437,447,489,508,634,663,752,856,896,992,1017,1038,1044,1060,1080,1160,1192,1220,1231,1309,1339,1368,1403,1505,1538,1553,1562,1601,1698,1715,1716,1770,1789,1855,1945,2077,2107,2132,2210,

The message was hidden at a randomly selected location using Red, Green, and Blue (RGB) colours identified using the Second Quotient Remainder Theorem (SQRT) formula. A pseudorandom number generator (PRNG) is a mechanism used to generate values or numbers assumed to be random. A series of numbers will be produced by PNRG that are not truly random but rather adhere to a predetermined algorithmic rule (Rani, Kurniawardhani, Angela, & Rendani, 2021).

The hiding process starts with generating a homophonic table and the dynamic representation (3D representation - x, y, z) of secret message characters using a PRNG random number generator. Subsequently, the secret message characters are mapped with RGB colour representation and concealed at random locations using PRNG. Finally, characters in the identified locations will be formatted with RGB colours representing hidden characters. The final result is a stego text file containing a hidden message. The RGB colour system is a combination of RGB values represented by values between (0,0,0) to (255,255,255). However, this study used the RGB values range between (0,0,0) to (15,15,15), producing a colour scale that is almost dark (black) compared to other values, as shown in Figure 5. Based on Figure 4, the values of RGBs between (0,0,0) to (15,15,15) show the changes in a dark colour, which are difficult to distinguish by human visuals compared to lighter colour changes (Mokrzycki & Tatol, 2011).

Figure 5

RGB Color Model



Based on Figure 5, RGB values exceeding (15,15,15) will significantly cause the colour palette to move away from dark colours. Therefore, a colour scale between (0,0,0) to (15,15,15) is an RGB colour scale close to dark colours. Alanazi, Zaidan, Zaidan, Jalab, and AL-Ani (2010), who studied steganographic images, stated that the RGB colour model is an essential technique used in computing to encode colour by representing it with various values. Previous studies have shown that the RGB colour range (0,0,0) to (15,15,15) is suitable for use in steganography text because it does not damage the generated visual document (Singh et al., 2014).

ANALYSIS AND RESULTS

This study used English texts as a medium for secret and covered text because different languages have different characters and frequencies of the characters. In this research, the characters of the secret message are represented with a random value so that it is more dynamic to allow repeated secret message characters to be represented with various values. Apart from that, a dynamic representation of the secret message is performed by generating a Homophonic table based on the frequency of characters in the cover text. Homophonic tables can represent secret message characters with various values, especially for repeating characters. The use of random techniques successfully produced various sets of secret messages, as shown in Table 3.

Table 3

Secret Message Representation Based on Homophonic Tables

	M	**E**	**E**	**T**	**Y**	**O**	**U**	**A**	**T**	**T**	**E**	**N**
C1	503	1968	81	1098	1590	287	1782	568	1477	682	1866	496
C2	1284	335	105	239	338	1032	1283	1131	1884	1914	1809	1953
C3	450	947	1864	11	1167	1534	1143	1313	366	1644	504	1691
C4	1285	297	1968	1981	1683	617	292	264	1884	293	995	595
C5	576	1014	361	1784	309	386	215	1681	607	340	1105	522
C6	730	1604	539	1922	794	1714	200	125	76	1055	1209	824

Table 3 presents the secret message characters “MEETYOUATTEN” represented with various values, as shown in C1, C2, C3, C4, C5 and C6. In addition, each repeating character can be represented with a different value. For example, the character ‘E’ for the second representation of C2 is represented by the values 577, 995 and 1809. These values will be converted to the form of (x, y, z) representation and mapped with Red, Green, and Blue (RGB) colour to perform the hiding process using Equation 2.

$$v = b\,(bx + y) + z, \tag{2}$$

where any value can represent the *b* variable. In this research, *b* = 15 assigns the maximum representation for x, y, and z not exceeding 15. Table 4 displays an example of the x, y and z representation for each character of the C2 value.

Table 4

Representation of x,y, and z values for the secret message

	M	**E**	**E**	**T**	**Y**	**O**	**U**	**A**	**T**	**T**	**E**	**N**
C2	1284	335	105	239	338	1032	1283	1131	1884	1914	1809	1953
x	5	1	0	1	1	4	5	5	8	8	8	8
y	10	7	7	0	7	8	10	0	5	7	0	10
z	9	5	0	14	8	12	8	6	9	9	9	3

As shown in Table 4, using the value of b = 15, character Y with the value of 338 can be represented with the values (1,7,8) and will be mapped with RGB colour (1,7,8) to format with the selected characters of the cover text. The random location is selected based on the value generated using the pseudorandom number generator (PRNG) for the hiding process. A sample of four secret message files has been selected to hide a secret message in the cover text labelled SMF1, SMF2, SMF3, and SMF4, as illustrated in Table 5 below.

Table 5

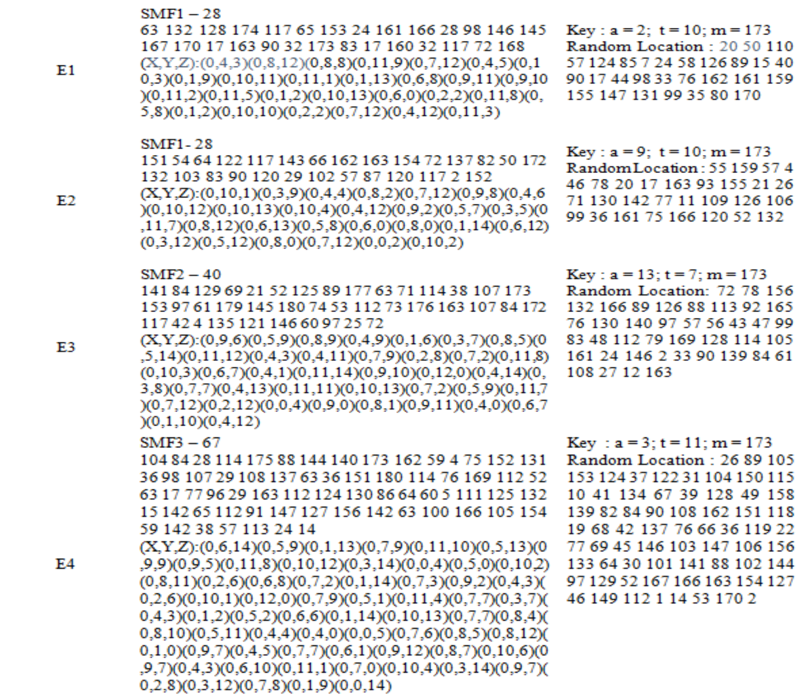
Sample of Secret Message Files

Code	The samples of the secrete messages	Size (character)
SMF1	ArrivedAtFebruaryTwentySeven	28
SMF2	Theimportanceandamountofdatahaveincrease	40
SMF3	TheCzechNationalBankbalanceofpayment figuresforthefirsthalfoftheyear	67
SMF4	Salzmannwhosaidhecannotbycontractretire fromthebankforatleastonemoreyearrejectsc hargesthathismembershipintheSenatewhile headingthecountrylargestbankinggroupwould constituteaconflictofinterestThereisnolegal requirementintheCchecRepublicforlegisla torstosuspendtheirbusiness	267

An experiment has been conducted by hiding the secret messages (SMF1, SMF2, SMF3) in the cover text CTF180. The results show that the characters of the secret messages have been successfully represented with the values of x, y, and z, as shown in Table 6. For example, in Experiment E1, a value of 63 and 132 were converted in (x,y,z) representation, yielding the value (0,4,3) and (0,8,12), respectively. Therefore, the character of the selected location in the cover text will be formatted with RGB colours by mapping with x,y and z values. The third column in Table 6 indicates the character at a random location, which will be formatted with an RGB colour map with the (x,y,z) value. For example, a character at locations 20 and 50 will be formatted with RGB colours (0,4,3) and (0,8,12), respectively.

Table 6

Representation of Secret Message (x,y,z) and its Random Locations



Experiment	Representation of secret message	Random Location
E1	SMF1 – 28 63 132 128 174 117 65 153 24 161 166 28 98 146 145 167 170 17 163 90 32 173 83 17 160 32 117 72 168 (X,Y,Z):(0,4,3)(0,8,12)(0,8,8)(0,11,9)(0,7,12)(0,4,5)(0,10,3)(0,1,9)(0,10,11)(0,11,1)(0,1,13)(0,6,8)(0,9,11)(0,9,10)(0,11,2)(0,11,5)(0,1,2)(0,10,13)(0,6,0)(0,2,2)(0,11,8)(0,5,8)(0,1,2)(0,10,10)(0,2,2)(0,7,12)(0,4,12)(0,11,3)	Key : a = 2; t = 10; m = 173 Random Location : 20 50 110 57 124 85 7 24 58 126 89 15 40 90 17 44 98 33 76 162 161 159 155 147 131 99 35 80 170
E2	SMF1 - 28 151 54 64 122 117 143 66 162 163 154 72 137 82 50 172 132 103 83 90 120 29 102 57 87 120 117 2 152 (X,Y,Z):(0,10,1)(0,3,9)(0,4,4)(0,8,2)(0,7,12)(0,9,8)(0,4,6)(0,10,12)(0,10,13)(0,10,4)(0,4,12)(0,9,2)(0,5,7)(0,3,5)(0,11,7)(0,8,12)(0,6,13)(0,5,8)(0,6,0)(0,8,0)(0,1,14)(0,6,12)(0,3,12)(0,5,12)(0,8,0)(0,7,12)(0,0,2)(0,10,2)	Key : a = 9; t = 10; m = 173 RandomLocation : 55 159 57 4 46 78 20 17 163 93 155 21 26 71 130 142 77 11 109 126 106 99 36 161 75 166 120 52 132
E3	SMF2 – 40 141 84 129 69 21 52 125 89 177 63 71 114 38 107 173 153 97 61 179 145 180 74 53 112 73 176 163 107 84 172 117 42 4 135 121 146 60 97 25 72 (X,Y,Z):(0,9,6)(0,5,9)(0,8,9)(0,4,9)(0,1,6)(0,3,7)(0,8,5)(0,5,14)(0,11,12)(0,4,3)(0,4,11)(0,7,9)(0,2,8)(0,7,2)(0,11,8)(0,10,3)(0,6,7)(0,4,1)(0,11,14)(0,9,10)(0,12,0)(0,4,14)(0,3,8)(0,7,7)(0,4,13)(0,11,11)(0,10,13)(0,7,2)(0,5,9)(0,11,7)(0,7,12)(0,2,12)(0,0,4)(0,9,0)(0,8,1)(0,9,11)(0,4,0)(0,6,7)(0,1,10)(0,4,12)	Key : a = 13; t = 7; m = 173 Random Location: 72 78 156 132 166 89 126 88 113 92 165 76 130 140 97 57 56 43 47 99 83 48 112 79 169 128 114 105 161 24 146 2 33 90 139 84 61 108 27 12 163
E4	SMF3 – 67 104 84 28 114 175 88 144 140 173 162 59 4 75 152 131 36 98 107 29 108 137 63 36 151 180 114 76 169 112 52 63 17 77 96 29 163 112 124 130 86 64 60 5 111 125 132 15 142 65 112 91 147 127 156 142 63 100 166 105 154 59 142 38 57 113 24 14 (X,Y,Z):(0,6,14)(0,5,9)(0,1,13)(0,7,9)(0,11,10)(0,5,13)(0,9,9)(0,9,5)(0,11,8)(0,10,12)(0,3,14)(0,0,4)(0,5,0)(0,10,2)(0,8,11)(0,2,6)(0,6,8)(0,7,2)(0,1,14)(0,7,3)(0,9,2)(0,4,3)(0,2,6)(0,10,1)(0,12,0)(0,7,9)(0,5,1)(0,11,4)(0,7,7)(0,3,7)(0,4,3)(0,1,2)(0,5,2)(0,6,6)(0,1,14)(0,10,13)(0,7,7)(0,8,4)(0,8,10)(0,5,11)(0,4,4)(0,4,0)(0,0,5)(0,7,6)(0,8,5)(0,8,12)(0,1,0)(0,9,7)(0,4,5)(0,7,7)(0,6,1)(0,9,12)(0,8,7)(0,10,6)(0,9,7)(0,4,3)(0,6,10)(0,11,1)(0,7,0)(0,10,4)(0,3,14)(0,9,7)(0,2,8)(0,3,12)(0,7,8)(0,1,9)(0,0,14)	Key : a = 3; t = 11; m = 173 Random Location : 26 89 105 153 124 37 122 31 104 150 115 10 41 134 67 39 128 49 158 139 82 84 90 108 162 151 118 19 68 42 137 76 66 36 119 22 77 69 45 146 103 147 106 156 133 64 30 101 141 88 102 144 97 129 52 167 166 163 154 127 46 149 112 1 14 53 170 2

Based on Table 6, SMF1 secret message'Arrived At February Twenty Seven" can be represented with different values and is hidden at different locations, as shown in the experiments. As an example, in experiment E1, a character at locations 20, 50, 110, 57, etc. will be formatted with RGB values (0,4,3), (0,8,12), (0,8,8), (0,11,9), etc. Experiment E2 refers that the same secret message, S1, has been formatted using a different RGB colour and locations but using the same cover text. It shows that a secret message can be hidden in different locations using the same cover text, resulting in various stego text. Other than that, different sizes of the secret message (SMF2, SMF3) also can be hidden in the same cover text as shown in Experiments E3 and E4, resulting in a different stego text. Figure 6 shows no difference between the cover text and stego text after the secret message "ArrivedAtFebruaryTwentySeven" has been hidden at a selected location. The generated stego text in Figure 6 did not show any suspicion compared to the suspicion stego text in Figures 3 and 4.

Figure 6

Generated Stego Text of the Proposed Study

Cover text	Stego text	Hidden location
Production at the huge nickel deposit at Voisey's Bay in remote Labrador is still years away, but already it risks falling behind schedule because of environmental concerns and pressure from aboriginal groups.Inco Ltd, the Toronto-based nickel giant that won control over the spectacular nickel, copper and cobalt property after a bidding war last spring, planned to start open pit production by 1998 and full-scale underground mining by 2000.	Production at the huge nickel deposit at Voisey's Bay in remote Labrador is still years away, but already it risks falling behind schedule because of environmental concerns and pressure from aboriginal groups. Inco Ltd, the Toronto-based nickel giant that won control over the spectacular nickel, copper and cobalt property after a bidding war last spring, planned to start open pit production by 1998 and full-scale underground mining by 2000.	6,30,126,137,181,357,315,147,221,144,209,96,17,74,302,95,13,58,238,212,108,65,266,324,183,365,347,275

The experiment results indicate that different secret message content can be hidden in different cover texts. Table 7 shows the maximum capacity of secret messages hidden in various sizes of cover text files.

Table 7

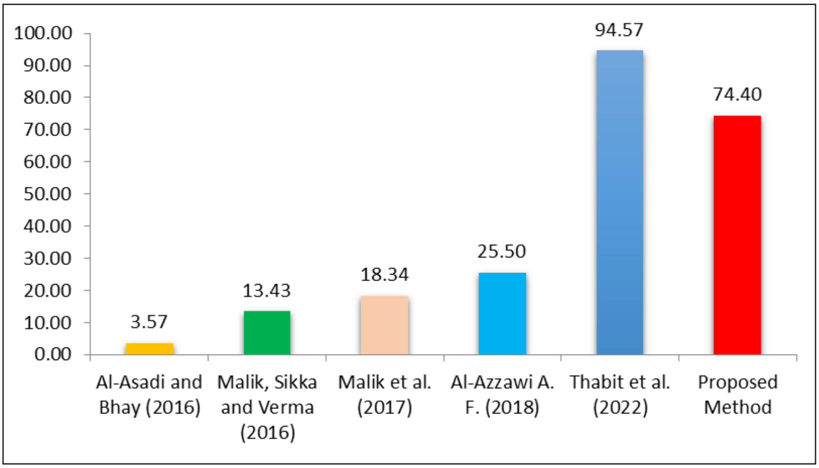
Maximum Capacity of Hidden Messages

Cover text files	Size of the cover text file	Size of the secret message file	Maximum hiding capacity
CTF180	180	116	64.4%
CTF243	243	183	75.3%
CTF376	376	283	75.3%
CTF847	847	660	78.9%
CTF1700	1700	1262	74.2%
CTF2153	2153	1958	90.9%
CTF2638	2638	2185	82.8%
		Average	**77.4%**

Table 7 presents the maximum size of the secret message that can be hidden in the cover text file. For example, CTF243 can hide a maximum of 183 secret message characters. Therefore, different sizes of cover text files can hide different sizes of secret messages. Table 7 shows that the average hiding capacity is 77.4%. On the other hand, Figure 7 demonstrated the percentage of hiding capacity using the RGB colour technique compared to the previous researchers.

Figure 7

Percentage of Hiding Capacity by the Previous Researchers



As a result, the RGB colour technique used in this study increased the hiding capacity up to 77.4% compared to other techniques, as shown in Figure 6. Although Thabit et al. (2022) can hide 94.57%, it produced a suspicious stego text, as shown in Figure 4. The generated Homorphonic table has successfully represented a secret message in various representations. Apart from that, this various representation technique is one of the advantages which is not implement by the previous researchers. These secret message values converted to 3D representation were mapped to RGB colour to meet the stated objective.

CONCLUSION AND FUTURE WORKS

This study successfully hides secret messages in a cover text by formatting cover text characters with Red, Green, and Blue (RGB) colours. The results demonstrate that a single secret message can be represented by multiple representations using the Second Quotient Remainder Theorem (SQRT) formula. Furthermore, RGB colour was utilised to format the character in a selected location to hide the secret message. The study presents that the hidden capacity increased compared to the previous study without a suspicious generated stego text. The proposed SQRT formula that converts the secret message into a three-dimensional (3D) representation can be applied to image steganography that uses an RGB colour to store a secrete message in the image pixel.

Instead, future research can be done by improving other characters, such as symbols, numbers and characters in the cover text, to overcome the available characters in the secret message. Using these characters could improve the hiding capacity because these characters are also available in most cover text and secret messages. Hence, hiding messages using a bit-level can be applied instead of using the character level to improve the hiding capacity.

ACKNOWLEDGMENT

I acknowledge that this paper is based on the research from my PhD thesis. Thanks to the School of Computing, University Utara Malaysia, for supporting me during my study.

REFERENCES

Agath, A., Sidpara, C., & Upadhyay, D. (2018). Critical Analysis of Cryptography and Steganography. *International Journal of Scientific Research in Science, Engineering and Technology*, *4*(2), 1–6.

Ahvanooey, M. T., Li, Q., Hou, J., Rajput, A. R., & Yini, C. (2019). Modern Text Hiding, Text Steganalysis, and Applications : A Comparative Analysis. *Entropy*, *21*(4), 1–29. https://doi.org/10.3390/e21040355

Al-Asadi, S. A., & Bhaya, W. (2016). Text Steganography in Excel Documents Using Color and Type of Fonts. *Research Journal of Applied Sciences*, *11*(10), 1054–1059.

Al-Azzawi, A. F. (2018). A Multi-Layer Hybrid Text Steganography For Secret Communication Using Word Tagging and RGB Color. *International Journal of Network Security & Its Applications*, *10*(6), 1–12. https://doi.org/10.5121/ijnsa.2018.10601

Alanazi, H. O., Zaidan, A. A., Zaidan, B. B., Jalab, H. A., & AL-Ani, Z. K. (2010). New Classification Methods for Hiding Information into Two Parts: Multimedia Files and Non Multimedia Files. *Journal of Computing*, *2*(3), 144–151. Retrieved from http://arxiv.org/abs/1003.4084

Alotaibi, R. A., & Elrefaei, L. A. (2018). Improved capacity Arabic text watermarking methods based on open word space. *Journal of King Saud University - Computer and Information Sciences*, *30*(2), 236–248. https://doi.org/10.1016/j.jksuci.2016.12.007

Arya, A., & Soni, S. (2018). A Literature Review on Various Recent Steganography Techniques. *International Journal on Future Revolution in Computer Science & Communication Engineering*, *4*(January), 143–149.

Atoum, M. S. (2018). Steganography and Watermarking : Review. *International Journal of Science and Research (IJSR)*, *7*(6), 2017–2019. https://doi.org/10.21275/ART20183644

Baawi, S. S., Mokhtar, M. R., & Sulaiman, R. (2018). A Comparative Study on The Advancement of Text Steganography Techniques in Digital Media. *ARPN Journal of Engineering and Applied Sciences*, *13*(5), 1854–1863.

Babu, K. R. (2010). A Survey on Cryptography and Steganography Methods for Information Security. *International Journal*, *12*(2), 13–17. https://doi.org/10.5120/1660-2235

Bhat, D., Prabhu, S., & Renuka, A. (2017). Information Hiding through Dynamic Text Steganography and Cryptography. In *International Conference on Advances in Computing, Communications and Informatics*, 1826–1831.

Dhavare, A., Low, R. M., & Stamp, M. (2013). Efficient Cryptanalysis of Homophonic Substitution Ciphers. *Cryptologia*, *37*(3), 37–41. https://doi.org/10.1080/01611194.2013.797041

Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. *Multimed Tools Appl*, *77*(13), 17333–17373.

Fabien A. P. Petitcolas, R. J. A. and M. G. K. (1999). Information Hiding – A Survey. In *Proceedings of the IEEE, special issue on protection of multimedia content*.

Jan, A., Parah, S. A., Hussan, M., & Malik, B. A. (2022). Double layer security using crypto - stego techniques : a comprehensive review. *Health and Technology*, 9–31. https://doi.org/10.1007/s12553-021-00602-1

Joseph, P., & Vishnukumar, S. (2015). A study on steganographic techniques. In *Global Conference on Communication Technologies, GCCT 2015* (pp. 206–210). https://doi.org/10.1109/GCCT.2015.7342653

Khan, Y., Algarni, A., Fayomi, A., & Almarashi, A. M. (2021). Disbursal of Text Steganography in the Space of Double-Secure Algorithm. *Hindawi Mathematical Problems in Engineering*, *2021*.

Kumar, R., Malik, A., Singh, S., & Chand, S. (2016). A high capacity Email based text steganography scheme using Huffman compression. *3rd International Conference on Signal Processing and Integrated Networks (SPIN) A*, 53–56.

Mahato, S., Khan, D. A., & Yadav, D. K. (2017). A Modified Approach to Data Hiding in Microsoft Word Documents by Change-Tracking Technique. *Journal of King Saud University Computer and Information Sciences*.

Majeed, M. A., & Sulaiman, R. (2021). A Review on Text Steganography Techniques. *Mathematics*, *9*.

Malik, A., Sikka, G., & Verma, H. K. (2016). A High Capacity Text Steganography Scheme Based on LZW Compression and Color Coding. *Engineering Science and Technology, an International Journal*, 4–11. https://doi.org/10.1016/j.jestch.2016.06.005

Malik, A., Sikka, G., & Verma, H. K. (2017). A High Capacity Text Steganography Scheme Based on Huffman Compression and Color Coding. *Journal of Information and Optimization Sciences, 38*(5), 647–664. https://doi.org/10.1080/02522667.2016.1197572

Maniriho, P., & Ahmad, T. (2017). A Data Hiding Approach Using Enhanced-RDE in Grayscale Images. In *2017 International Conference on Advanced Mechatronics, Intelligent Manufacture, and Industrial Automation (ICAMIMIA)* (pp. 35–40). IEEE.

Mokrzycki, W., & Tatol, M. (2011). Color difference Delta E - A survey. *Machine Graphics and Vision*, (April 2011), 383–411.

Patel, P., & Patro, S. P. (2017). Analysis of Information Security through Crypto-Stenography with Reference to E-Cipher Methods. *International Journal of Advanced Research in Computer and Communication Engineering*, *6*(11), 332–336. https://doi.org/10.17148/IJARCCE.2017.61158

Por, L. Y., & Delina, B. (2008). WhiteSteg: A New Scheme in Information Hiding Using Text Steganography. *7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science (ACACOS)*, *7*(6), 689–695. Retrieved from http://www.wseas.us/e-library/conferences/2008/hangzhou/acacos/116-586-634.pdf

Pujari, A. A., & Shinde, S. S. (2016). Data Security using Cryptography and Steganography. *IOSR Journal of Computer Engineering*

(IOSR-JCE), *18*(4), 130–139. https://doi.org/10.9790/0661-180405130139

Rani, S., Kurniawardhani, A., Angela, Y., & Rendani, W. (2021). Steganography on Digital Color Image Using Modulo Function and Pseudorandom Number Generator. *International Journal on Advanced Science Engineering Information Technology*, *11*(6), 2470–2475.

Rasmi, A., & Mohanapriya, M. (2016). An Extensive Survey of Data Hiding Techniques. *Indian Journal of Science and Technology*, *9*(28), 1–7. https://doi.org/10.17485/ijst/2016/v9i28/90457

Shivani, Yadav, V. K., & Batham, S. (2015). A Novel Approach of Bulk Data Hiding using Text Steganography. *Procedia Computer Science*, *57*, 1401–1410. https://doi.org/10.1016/j.procs.2015.07.457

Singh, H., Diwakar, A., & Upadhyaya, M. S. (2014). A Novel Approach to Text Steganography. In *International Congress on Computer, Electronics, Electrical, and Communication Engineering*, 59, 7–12. https://doi.org/10.7763/IPCSIT.2014.V59.2

Stojanov, I., Mileva, A., & Stojanovi, I. (2014). A New Property Coding in Text Steganography of Microsoft Word Documents A New Property Coding in Text Steganography of Microsoft Word Documents. In *SECURWARE 2014 : The Eighth International Conference on Emerging Security Information, Systems and Technologies*.

Tang, X., & Chen, M. (2013). Design And Implementation Of Information Hiding System Based On RGB. In *IEEE-3rd International Conference on Consumer Electronics, Communications and Networks*, 217–220.

Thabit, R., Udzir, N. I., Yasin, S., Asmawi, A., & Gutub, A. (2022). CSNTSteg : color spacing normalisation text steganography model to improve capacity and invisibility of hidden data. *IEEE Access*, *PP*, 1. https://doi.org/10.1109/ACCESS.2022.3182712

Wang, X., & Li, H. (2014). Research on Information Hiding Method Based on Word Text. *Advanced Materials Research*, *930*, 2815–2818. https://doi.org/10.4028/www.scientific.net/AMR.926-930.2815

Zhang, J., Huang, H., Wang, L., Lin, H., & Gao, D. (2017). Coverless Text Information Hiding Method Using the Frequent Words Hash. *International Journal of Network Security*, *19*(6), 1016–1023. https://doi.org/10.6633/IJNS.201711.19(6).18

Zielińska, E., Mazurczyk, W., & Szczypiorski, K. (2014, March). Trends in Steganography. *Communications of the ACM*, *57*(3), 86–95. https://doi.org/10.1145/2566590.2566610